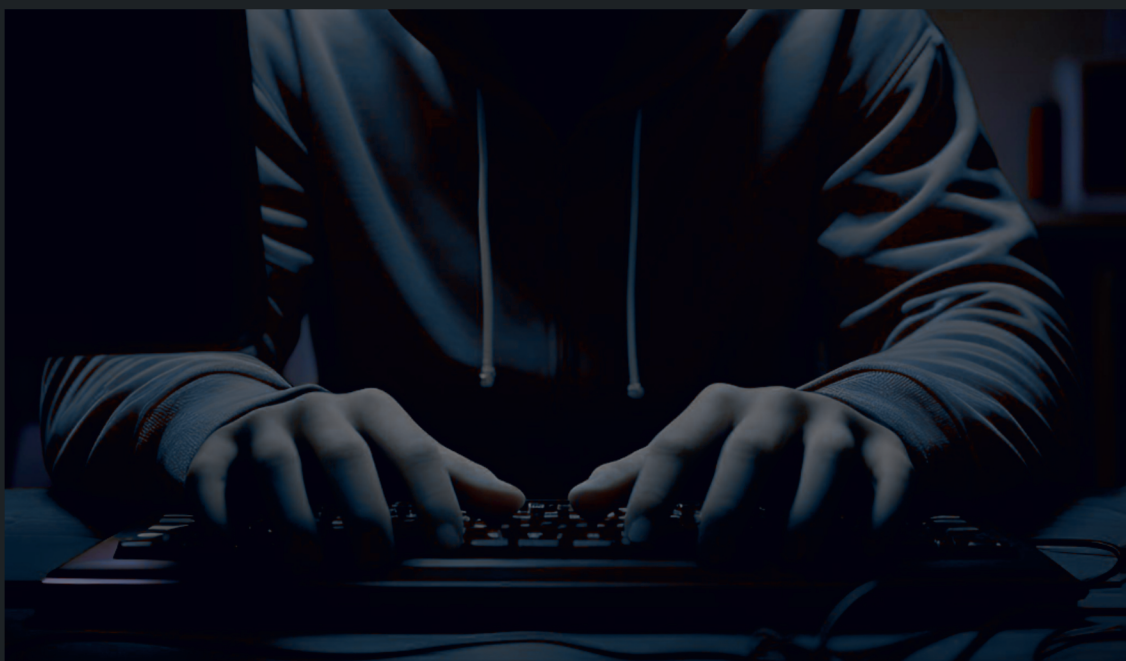


Kinga Pázmándi – Renáta Hrecska-Kovács (eds.)

CYBERBULLYING, HATE CRIME AND RELATED ISSUES FROM A COMPARATIVE PERSPECTIVE



STUDIES OF THE FERENC MÁDL
INSTITUTE





STUDIES OF THE FERENC MÁDL INSTITUTE

HU ISSN 2939-5542

EDITOR-IN-CHIEF OF THE SERIES:

Zsuzsa Wopera, President of the Ferenc Mádl Institute of Comparative Law,
Professor Faculty of Law University of Miskolc

SERIES EDITORIAL BOARD:

Kinga Pázmándi, Vice-President of the Ferenc Mádl Institute of Comparative Law,
Associate Professor, Head of Department, Faculty of Economics, ELTE

Erika Herédi, Head of Department, Ferenc Mádl Institute of Comparative Law,
Associate Professor, Faculty of Law, Széchenyi University

Adrienn Nagy, Head of Department, Ferenc Mádl Institute of Comparative Law,
Associate Professor, Director of Institute, Faculty of Law, University of Miskolc

Julianna Sára Traser, Head of Department, Ferenc Mádl Institute of Comparative Law

BOOK SERIES MANAGER:

Istvánné Szabó Head of Department, Head of Secretariat,
Ferenc Mádl Institute of Comparative Law

The book series *Studies of the Ferenc Mádl Institute* seeks to publish the most significant and intriguing results of the researches conducted by colleagues of the Ferenc Mádl Institute of Comparative Law in English. The primary goal of the series is to authentically present and address legal issues which arise related to the Central and Eastern European region, taking into account the particular legal traditions and culture of the countries therein. Therefore this series is a good platform to cooperate with Central European Academy. The series also aims to provide insights and detailed analyses of certain legal topics regarding the countries outside the Central and Eastern European region. Furthermore its purpose to encompass titles which are monographic studies of the researchers of Ferenc Mádl Institute of Comparative Law. The books published in the series are written for both academics and legal practitioners who are interested in contemporary legal problems related to Central and Eastern European countries.

CYBERBULLYING, HATE CRIME
——— AND RELATED ISSUES ———
FROM A COMPARATIVE PERSPECTIVE

Kinga Pázmándi –
Renáta Hrecska-Kovács
(eds.)



FERENC MÁDL INSTITUTE OF COMPARATIVE LAW
Budapest • 2025

Kinga Pázmándi – Renáta Hrecska-Kovács (eds.)
**CYBERBULLYING, HATE CRIME AND RELATED ISSUES
FROM A COMPARATIVE PERSPECTIVE**

PUBLISHED BY
© Ferenc Mádl Institute of Comparative Law
H-1054 Budapest, Báthory str. 10.
Zsuzsa Wopera, Head of Institute

ISBN 978-615-6356-49-9
ISBN 978-615-6356-50-5 (pdf)
<https://doi.org/10.47079/2025.kprhk.cyberb.4>

The manuscript has been closed in January 2025; the cited websites were accessed between
1 December 2024 and 31 January 2025.

COVER DESIGN:
Gyöngyi Kovács

LAYOUT:
Idea Plus (Elemér Könczey, Botond Fazakas)
Cluj-Napoca, Romania

CONTRIBUTORS

EDITORS

Kinga Pázmándi

Vice-President of the Ferenc Mádl Institute of Comparative Law

Associate Professor, Head of Department, Faculty of Economics, ELTE

Dr. Renáta Hrecska-Kovács PhD, LL.M.

Senior Researcher, Ferenc Mádl Institute of Comparative Law

AUTHORS

Dr. Nóra Béres PhD, LL.M.

senior researcher, Ferenc Mádl Institute of Comparative Law

assistant professor, University of Miskolc, Faculty of Law, Institute of European and International Law, Department of International Law

Dr. Erika Váradi-Csema PhD, LL.M.

associate professor, University of Miskolc, Faculty of Law, Institute of Criminal Sciences

president of Interdisciplinary Research Center for Alternative Conflict Solution and Dispute Resolution, University of Miskolc, Faculty of Law

Dr. Márta Sarolta Deák

researcher, Ferenc Mádl Institute of Comparative Law

Dr. Laura De Negri PhD, LL.M.

researcher, Ferenc Mádl Institute of Comparative Law

CONTRIBUTORS

Dr. László Dornfeld

senior analyst, Center for Fundamental Rights

Co-President, PhD Section of the Hungarian Society of Criminology

Dr. Dávid Hojnyák

assistant professor, University of Miskolc, Faculty of Law, Institute of Legal History and Legal Theory, Department of Legal Theory and Sociology of Law

Dr. Attila Horváth PhD

senior researcher, Ferenc Mádl Institute of Comparative Law

associate professor, Faculty of Political Sciences and International Studies, National University of Public Service, Department of Constitutional Law and Comparative Public Law

Prof. Dr. Nóra Jakab PhD

professor, University of Miskolc, Faculty of Law, Institute of Private Law, Department of Labour and Agricultural Law

Dr. habil. Ágnes Juhász PhD

senior researcher, Ferenc Mádl Institute of Comparative Law

associate professor, University of Miskolc, Faculty of Law, Institute of Private Law, Department of Civil Law

Dr. Roland Lindt LL.M.

PhD student, University of Miskolc, Ferenc Deák Doctoral School of Law

assistant professor, University of Miskolc, Faculty of Law, Institute of Public Law, Department of Constitutional Law

Dr. György Marinkás PhD

senior researcher, Ferenc Mádl Institute of Comparative Law

associate professor, University of Miskolc, Faculty of Law, Institute of European and International Law, Department of European Law and International Private Law

Prof. Dr. Zoltán Nagy PhD

professor, Head of Department of Financial Law, University of Miskolc, Faculty of Law, Institute of Political Sciences

Dr. Zoltán Németh LL.M.

researcher, Ferenc Mádl Institute of Comparative Law

CONTRIBUTORS

Dr. Gabriel Stollsteiner
researcher, Ferenc Mádl Institute of Comparative Law

Dr. Pál Szentpáli-Gavallér
researcher, Ferenc Mádl Institute of Comparative Law
PhD student, University of Miskolc, Ferenc Deák Doctoral School of Law

Dr. János Szinek LL.M.
PhD Candidate, Ferenc Deák Doctoral School of Law, Faculty of Law, University of Miskolc

Dr. Péter Szőke
senior researcher, Ferenc Mádl Institute of Comparative Law

Dr. Álmos Ungvári
PhD Candidate, Peter Pazmany Catholic University, Faculty of Law and Political Sciences

REVIEWERS

Dr. Bartłomiej Oręziak PhD
Cardinal Stefan Wyszyński University in Warsaw, Poland

dr. Andras Bethlendi
Sapientia Hungarian University of Transylvania, Cluj-Napoca, România

Dr. Gábor Hulkó PhD
Széchenyi István University of Győr, Hungary

Kathrin Stiebellehner (post doc)
Johannes Kepler Universität Linz, Austria

Dr. Gabriella Kulcsár PhD
University of Pécs, Faculty of Law, Hungary

doc. PhDr. JUDr. Lilla Garayová, PhD, LL.M.
Paneuropean University, Bratislava, Slovakia

CONTRIBUTORS

Dr. Kitti Mezei PhD

Institute of Legal Studies, Budapest, Hungary

Miikka Vuorela PhD

University of Eastern Finland, Law School, Faculty of Social Sciences and Business Studies, Joensuu / Kuopio, Finland

Dr. Peter Coe

Birmingham Law School, University of Birmingham, United Kingdom

Dr. Péter Sereg, LL.M., PhD

Ferenc Mádl Institute of Comparative Law

Valérie Nicolas

Université Paris Nanterre, Centre for the Theory and Analysis of Law, Nanterre, France

Vincenzo Carbone

Rome Bar Association; University of International Studies of Rome, Italy; WU Vienna University of Economics and Business, Vienna, Austria

Dr. habil. Zsolt Zódi PhD

Ludovika University of Public Service, Institute of the Information Society, Budapest, Hungary

Dr. Noémi Suri PhD

Ferenc Mádl Institute of Comparative Law

BRIEF TABLE OF CONTENTS

List of Abbreviations	19
<i>Roland Lindt</i> , Introduction – Idea, Concept, Structure and Methodology	21
<i>Zoltán Nagy</i> , I. Challenges of Technological Development for the Legal Development	27
<i>László Dornfeld – Erika Váradi-Csema</i> , II. In the Grip of a Changing World – Conceptual and Formal Approaches	41
<i>Erika Váradi-Csema</i> , III. At Intersection of Disciplines – The Justification of a Holistic Approach.	53
<i>Nóra Béres</i> , IV. Online Hate Speech, Cyberbullying and the Echtr: Toward a Common European Standard?	75
<i>Roland Lindt – György Marinkás</i> , V. Progress Report 2024 on the Never-Ending War – An Overview of EU Law Against Deviances Induced by Hatred in the Online Space.	99
<i>Erika Váradi-Csema – László Dornfeld – Roland Lindt</i> , VI. <i>Qui Non Vetat Peccare, Cum Possit, Iubet</i> – The Case Of Hungary And Hostility Online	139
<i>Dávid Hojnyák</i> , VII. Hate Speech and Cyberbullying in Czech Law.	179
<i>Márta Sarolta Deák</i> , VIII. Hate Speech and Cyberbullying in the Polish Legal Regulation	203
<i>Pál Szentpáli-Gavallér</i> , IX. To Hate or not to Hate – Regulation of Hate Speech and Cyberbullying in Romania.	227
<i>János Szineck</i> , X. Regulation of Digital Offences in the 21 st Century with Special Regard to the Crime of Dangerous Electronic Harassment in Slovakia	251
<i>De Negri Laura</i> , XI. Regulatory Issues of Hate Speech in Austria – An Exemplary Regulatory Model in Europe	277

BRIEF TABLE OF CONTENTS

<i>Nóra Jakab</i> , XII. The Legal Approach of Cyberbullying in Germany	309
<i>Zoltán Németh</i> , XIII. Denmark – Future-Proof Provisions in the Fight Against Cyberbullying	341
<i>Zoltán Németh</i> , XIV. Finland: where Prevention Starts in Schools.	371
<i>Ágnes Juhász</i> , XV. Hate Speech, Cyberbullying and the Difficulty of Detecting Crime in Online Space – The Example of the United Kingdom . . .	401
<i>Attila Horváth</i> , XVI. New Challenges, new Laws: Tackling Hate Crimes and Cyberbullying in Ireland	437
<i>Gabriel Stollsteiner</i> , XVII. Hate Speech and Cyberbullying in Belgium: Critical Update Required	477
<i>Péter Szőke</i> , XVIII. Liberté, Égalité... Et Fraternité? Combating Hate Speech and Cyberbullying in France, Home of the Enlightenment. . . .	505
<i>Álmos Ungvári</i> , XIX. Hate Speech and Cyberbullying in Italy	547

TABLE OF CONTENTS

LIST OF ABBREVIATIONS	19
INTRODUCTION – IDEA, CONCEPT, STRUCTURE AND METHODOLOGY	21
Bibliography	25
I. CHALLENGES OF TECHNOLOGICAL DEVELOPMENT FOR THE LEGAL DEVELOPMENT	27
Bibliography	38
II. IN THE GRIP OF A CHANGING WORLD – CONCEPTUAL AND FORMAL APPROACHES	41
1. Conceptual diversity: from bullying to cyberbullying	42
2. Criminological aspects of the use of the term	46
3. Hate speech and cyberbullying	47
Summary	50
Bibliography	51
III. AT INTERSECTION OF DISCIPLINES – THE JUSTIFICATION OF A HOLISTIC APPROACH	53
1. Cyberbullying	53
2. Causes and effects	58
3. Focus on hate speech	63
4. Perpetrators and victims	65
Summary	68
Bibliography	69
IV. ONLINE HATE SPEECH, CYBERBULLYING AND THE ECtHR: TOWARD A COMMON EUROPEAN STANDARD?	75
1. Introduction	75
2. Online hate speech in the case-law of the ECtHR.	76
2.1. <i>General overview: hate speech in international law</i>	76
2.2. <i>Hate speech in Strasbourg case-law: a general framework</i>	79
2.3. <i>The specifics of online hate speech in Strasbourg case-law</i>	83
3. Cyberbullying in the case-law of the ECtHR.	90
Summary	95
Bibliography	97

V. PROGRESS REPORT 2024 ON THE NEVER-ENDING WAR – AN OVERVIEW

OF EU LAW AGAINST DEVIANCES INDUCED BY HATRED IN THE ONLINE SPACE 99

1. Introductory Thoughts on the Beginnings of the Fight Against Hatred .	99
2. Harmonisation of Hate Crime in the EU	104
2.1. <i>Legal Basis of Criminal Law Harmonisation in EU's Primary Law</i> . . .	104
2.2. <i>The Joint Action Concerning Action to Combat Racism and Xeno-phobia.</i>	106
2.3. <i>Criminal Law Harmonisation of Our Days: Main Provisions of the Council Framework Decision.</i>	107
2.4. <i>Evaluation of the Situation of Hate Crime in the EU – Chal-lenges of the Near Future</i>	110
3. Cyberbullying – Tackling the Issue of Cyberbully with ‘Non-Cyberbully Specific’ EU Legal Framework and Some Related Policies.	111
3.1. <i>EU Legal Frameworks and Policies</i>	111
3.2. <i>Other Approaches</i>	116
4. Child Protection in the Digital Age ‘from the Digital Age’ – EU Perspective	118
5. The Beginning of a New Age of platform liability (?): Main Rules of DSA.	122
5.1. <i>The ‘Ante DSA Era’ – Relevant Provisions of the E-Commerce Directive</i>	123
5.2. <i>The structure and the main novelties of DSA</i>	125
5.3. <i>Expectations and Misgivings</i>	129
Summary	130
<i>Final Thoughts on the Status Quo of EU Legislation vs. Deviances Induced by Hatred</i>	130
Bibliography	132

VI. QUI NON VETAT PECCARE, CUM POSSIT, IUBET – THE CASE OF HUNGARY

AND HOSTILITY ONLINE. 139

1. Introductory Thoughts	139
1.1. <i>The Constitution of the Hungarian People's Republic and Funda-mental Rights (1949–2011)</i>	140
1.2. <i>The Constitutional Foundations of the Freedom of Expression Today: The Fundamental Law of Hungary</i>	144
2. Regulation of Hate Speech	145
2.1. <i>History of Incitement Against the Community</i>	146
2.2. <i>Current Regulation of Hate Speech and Related Offences</i>	148
2.3. <i>Future Perspectives – Definition of Aggression on Internet.</i>	150
2.4. <i>A Civil Law Tool Against Hate Speech</i>	151
3. Regulation of cyberbullying.	151
3.1. <i>Harassment</i>	152
3.2. <i>Relationship violence</i>	154

TABLE OF CONTENTS

3.3. Humiliation of a vulnerable person	155
3.4. Assisting a suicide	157
3.5. Defamation and Insult	158
3.6. False audio or video recording	160
3.7. Other Offences	160
4. Focus on Prevention and Particularly Vulnerable Groups	161
4.1. From the Digital Strategy for Child Protection to the National Crime Prevention Strategy	163
4.2. Professional Events, Organisational Initiatives	165
4.3. General and Specific Programs to Combat (Cyber)bullying	166
4.4. Campaigns, Other Initiatives, Immediate Help Solutions	170
5. Responsibility of Service Providers	172
5.1. A New Dawn – Liability of Service Providers Since DSA	173
Summary	174
Bibliography	175
VII. HATE SPEECH AND CYBERBULLYING IN CZECH LAW	179
1. Hate speech in Czech law	179
1.1. Defamation of a national, racial, ethnic or other group of persons	180
1.2. Incitement to hatred against a group of persons or incitement to restrict their rights and freedoms	180
1.3. Violence against a group of people and an individual	181
1.4. Other offences	181
2. Regulation of (cyber)bullying in Czech law	186
2.1. Concepts of cyberbullying in Czech criminal law	186
3. Prevention legislation and practice	193
4. The issue of service provider liability for offences committed in the online space	195
Summary	199
Bibliography	201
VIII. HATE SPEECH AND CYBERBULLYING IN THE POLISH LEGAL REGULATION	203
1. Introduction	203
2. Regulatory Issues on Hate Speech	203
2.1. Freedom of Expression and its Limitations	203
2.2. Hate Speech Regulations	205
3. The Regulation of Cyberbullying	208
3.1. Regulatory Framework	208
3.2. Legal Practice	213
3.3. Abuse at Work or in an Educational Institution	214
3.4. The Connection Between Cyberbullying and Hate Speech	216

TABLE OF CONTENTS

4. Preventive Legislation and Practice	216
5. The Responsibility of Service Providers and Institutions	219
Summary	223
Bibliography	225
 IX. TO HATE OR NOT TO HATE – REGULATION OF HATE SPEECH AND CYBERBULLYING IN ROMANIA.....	
1. Introduction.....	227
2. Regulatory issues of hate speech	228
2.1. <i>Definition of hate speech in Romania, related case law</i>	228
2.2. <i>Statistics on hate speech in Romania</i>	234
3. About Romanian cyberbullying.....	235
4. Practice related to prevention	240
5. Liability of service providers and institutions	244
Summary	245
Bibliography	249
 X. REGULATION OF DIGITAL OFFENCES IN THE 21ST CENTURY WITH SPECIAL REGARD TO THE CRIME OF DANGEROUS ELECTRONIC HARASSMENT IN SLOVAKIA	
1. Regulatory aspects of hate speech.....	251
2. Cyberbullying in Slovakia.....	254
2.1. <i>Bullying at schools</i>	258
2.2. <i>Bullying at work</i>	260
3. Legislation on prevention and case law	262
4. Responsibilities of service providers and institutions.....	265
4.1. <i>Responsibilities of educational institutions</i>	268
4.2. <i>Responsibility of the employer</i>	269
Summary	271
Bibliography	274
 XI. REGULATORY ISSUES OF HATE SPEECH IN AUSTRIA – AN EXEMPLARY REGULATORY MODEL IN EUROPE.....	
1. Hate speech and constitutional background – fundamental rights and cyberbullying in Austria	277
2. The regulation method of cyberbullying in Austria.....	278
2.1. <i>Hate speech in the offline space</i>	279
2.2. <i>Hate speech in the online space</i>	283
2.3. <i>Hate speech in judicial practice</i>	285
3. Regulation of cyberbullying.....	286
3.1. <i>Implementation of cyberbullying into the Austrian StGB</i>	286
3.2. <i>Analysis of the facts</i>	289

TABLE OF CONTENTS

3.3. <i>Specific characteristics of the offence</i>	290
4. Enforceability of official action against online crime, cyberbullying and hate speech	294
4.1. <i>The monitoring procedure</i>	295
4.2. <i>Cases of fines.</i>	296
4.3. <i>Preventive legislation and practice.</i>	298
4.4. <i>No hate speech movement.</i>	298
5. Responsibilities of service providers and institutions.	300
5.1. <i>Reporting obligations for service providers.</i>	301
5.2. <i>Responsible agent and authorised agent for notification</i>	303
5.3. <i>Enforcement.</i>	303
Summary	304
Bibliography	306
XII. THE LEGAL APPROACH OF CYBERBULLYING IN GERMANY	309
Introduction.	309
1. Analysis of the Penal Code	312
2. Factual elements of certain hate crimes	316
2.1. <i>Hate-mongering insult</i>	319
2.2. <i>Stalking</i>	321
2.3. <i>Cybercrime</i>	323
2.4. <i>Action against online hate crime, service provider responsibility.</i>	324
3. Protection of minors	329
4. Prevention	333
Summary	336
Bibliography	338
XIII. DENMARK – FUTURE-PROOF PROVISIONS IN THE FIGHT AGAINST CYBERBULLYING	341
1. Regulatory issues of hate speech	341
1.1. <i>The relationship between freedom of expression and hate speech</i>	346
1.2. <i>Findings</i>	348
2. Regulation of cyberbullying.	348
2.1. <i>Cybercrime in general in Denmark</i>	348
2.2. <i>Danish regulation of cyberbullying.</i>	349
2.3. <i>Cyberbullying in the workplace.</i>	350
2.4. <i>Cyberbullying rules in the Danish Criminal Code.</i>	352
2.5. <i>Protection of personal data and its relation to cyberbullying</i>	355
2.6. <i>Prevalence of online bullying in Danish educational institutions.</i>	355
2.7. <i>Remarks</i>	358
3. Regulation and practice related to prevention	358
3.1. <i>Prevention in schools</i>	358
3.2. <i>Findings</i>	361

TABLE OF CONTENTS

4. Responsibility of service providers and institutions	362
4.1. <i>Responsibility of service providers</i>	362
4.2. <i>Responsibility of educational institutions</i>	363
4.3. <i>Responsibility of workplaces.</i>	365
4.4. <i>Remarks.</i>	365
Summary	366
Bibliography	369
XIV. FINLAND: WHERE PREVENTION STARTS IN SCHOOLS.	371
1. Hate speech regulation issues	371
1.1. <i>The hate speech.</i>	371
1.2. <i>The limits of freedom of expression in the context of hate crimes</i>	374
1.3. <i>Statistics.</i>	376
1.4. <i>Preventing hate speech</i>	377
1.5. <i>Summary</i>	378
2. Regulation of cyberbullying	380
2.1. <i>Cyberbullying in the Finnish Criminal Code.</i>	381
2.2. <i>Cyberbullying in the workplace.</i>	382
2.3. <i>Cyberbullying in schools.</i>	385
2.4. <i>Summary</i>	387
3. Regulation and practice related to prevention	387
3.1. <i>Prevention in educational institutions.</i>	387
3.2. <i>Recommendations of the working group for more effective action</i> <i>against hate speech and cyberbullying</i>	391
3.3. <i>Summary</i>	392
4. Responsibility of service providers and institutions	393
4.1. <i>Responsibility of service providers</i>	393
4.2. <i>Employers.</i>	395
4.3. <i>Educational institutions</i>	396
4.4. <i>Summary</i>	397
Bibliography	399
XV. HATE SPEECH, CYBERBULLYING AND THE DIFFICULTY OF DETECTING CRIME IN ONLINE SPACE – THE EXAMPLE OF THE UNITED KINGDOM	401
1. Regulation of hate speech.	401
1.1. <i>England, Scotland, and Wales</i>	402
1.2. <i>Northern Ireland</i>	408
2. Definition and regulation of cyberbullying	410
3. Regulation and prevention of bullying and cyberbullying at the workplace and at the school.	421
3.1. <i>Bullying and cyberbullying at the workplace</i>	421
3.2. <i>Bullying and cyberbullying at the workplace</i>	423

TABLE OF CONTENTS

4. Crimes committed in the online space, cyberbullying, and the enforceability of the authorities' action against hate speech	426
5. The liability of internet service providers and social media platforms	428
Bibliography	434
XVI. NEW CHALLENGES, NEW LAWS: TACKLING HATE CRIMES AND CYBERBULLYING IN IRELAND	437
1. The legal dimensions of hate speech and hate crime.	437
1.1. <i>The 1989 Prohibition of Incitement to Hatred Act and its critics.</i>	437
1.2. <i>Re-regulating hate crimes: the Criminal Justice (Hate Offences) Act 2024</i>	444
2. Fighting cyberbullying: unpacking the toolbox	448
2.1. <i>Victims and offenders in the light of researches.</i>	448
2.2. <i>The legal background</i>	451
2.3. <i>New act on online harassment: necessary but not sufficient?</i>	455
2.4. <i>Safe even online? The Online Safety and Media Regulation Act 2022</i> . .	461
3. From school policies to hotlines: ways of prevention	464
Summary	469
Bibliography	471
XVII. HATE SPEECH AND CYBERBULLYING IN BELGIUM: CRITICAL UPDATE REQUIRED	477
1. 'Censorship can never be introduced': Belgium's constitutional background	477
2. Hate speech and the persistence of de facto impunity.	478
2.1. <i>Hate speech's splintered legal background.</i>	479
2.2. <i>Press offense and its impact on hate speech laws' enforceability.</i>	483
2.3. <i>Harassment, cyberbullying and related offenses</i>	488
3. Preventing hate speech and (cyber)bullying: organisations and public policies	491
3.1. <i>From prevention to reparation: the role of public organisations</i>	491
3.2. <i>Prevention in schools: the case of the French Community</i>	494
3.3. <i>Platform liability and the case of cascading liability (responsabilité en cascade).</i>	497
Summary	500
Bibliography	502
XVIII. LIBERTÉ, ÉGALITÉ... ET FRATERNITÉ? COMBATING HATE SPEECH AND CYBERBULLYING IN FRANCE, HOME OF THE ENLIGHTENMENT	505
1. Striking a delicate balance: hate speech in physical and virtual space	505
1.1. <i>Introductory remarks: to punish or not to punish.</i>	505
1.2. <i>From Voltaire to anti-racist legislation.</i>	507

TABLE OF CONTENTS

1.3. <i>New minorities: extending protection in post-colonial France</i>	510
1.4. <i>New fronts open up: the battle continues in cyberspace</i>	513
1.5. <i>The rules in force</i>	516
1.6. <i>Hate speech between penal law and press law</i>	518
1.7. <i>Hate speech in a volatile jurisprudence</i>	519
2. <i>Cyberbullying: sui generis offences vs. qualifying circumstances</i>	524
2.1. <i>Digitalization of criminal offences</i>	524
2.2. <i>Moral harassment at work, at home, at school... anywhere</i>	527
3. <i>Right to a harassment-free environment</i>	530
4. <i>Liability: service providers and institutions in a ‘cascade’</i>	534
4.1. <i>From printed press to social media: editorial responsibility sublimating</i>	534
4.2. <i>Addressing constitutional limits to immediate removal of illegal content</i>	535
4.3. <i>Collaboration of the platforms with users and authorities</i>	538
4.4. <i>Compromises in the current liability regime</i>	539
4.5. <i>Competence and jurisdiction</i>	541
Summary	542
Bibliography	544
XIX. HATE SPEECH AND CYBERBULLYING IN ITALY	547
Introduction	547
1. <i>Hate Speech Regulation</i>	547
2. <i>Regulation of Cyberbullying</i>	554
2.1. <i>The instruments provided by the Act No. 71. of 2017 to fight cyberbullying</i>	560
2.2. <i>Criminal law relevance of cyberbullying</i>	563
3. <i>Prevention of Cyberbullying</i>	565
4. <i>Prevention and Responsibilities of Service Providers and Schools</i>	568
Summary	570
Bibliography	572

LIST OF ABBREVIATIONS

ABCPA – Anti-social Behaviour, Crime, and Policing Act, 2014 (United Kingdom)	EECC – European Electronic Communications Code
AI – Artificial Intelligence	ENABLE – European Network Against Bullying in Learning and Leisure Environments
ARCOM – Audio-visual and Digital Communications Regulatory Authority (France)	ENOC – European Network of Ombudsmen for Children
AVMSD – Audiovisual Media Services Directive	EPP – European People's Party Group
BIK+ – Better Internet for Children Strategy 2022	EU – European Union
BzKJ – Federal Centre for the Protection of Children and Young People (Bundeszentrale für Kinder- und Jugendmedienschutz, Germany)	FRA – European Agency for Fundamental Rights
CCRX – Consultative Commission on Racism and Xenophobia	GDPR – General Data Protection Regulation
CFA – Children First Act 2015 (Ireland)	GG – Grundgesetz für die Bundesrepublik Deutschland
CJEU – Court of Justice of the European Union	GTC – General Terms and Conditions
ČŠI – Czech School Inspectorate	HHCROA – Harassment, Harmful Communications and Related Offences Act 2020 (Ireland)
CVTI SR – Centrum vedecko-technických informácií Slovenskej republiky (Scientific and Technical Information Centre of the Slovak Republic)	HiNBG – Hass-im-Netz-Bekämpfungsgesetz (Austria)
DAS – Digital Services Act (Germany)	HOA – Criminal Justice (Hate Offences) Act 2024 (Ireland)
DCUM – Dansk Center for Undervisningsmiljø (Danish Center for Educational Environment)	IBSA – Image-Based Sexual Abuse
DEP – European Union's Digital Europe Programme	ICCPR – International Covenant on Civil and Political Rights
DIGITAL – European Union's Digital Europe Programme	ICCPR – International Covenant on Civil and Political Rights
DMA – Digital Markets Act	ICERD – International Convention on the Elimination of All Forms of Racial Discrimination adopted in New York on 21 December 1965
DSA – Digital Service Act	ICT – Information and Communication Technology
DSC – Digital Services Coordinator	IFDH – Federal Institute for Human Rights (Belgium)
ECD – E-Commerce Directive	INDH – National Institute for Human Rights (Belgium)
ECHR – European Convention on Human Rights	IVHHO Bill – Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 (Ireland)
ECRI – European Commission against Racism and Intolerance	
ECtHR – European Court of Human Rights	
EDRI – European Digital Rights network	

LIST OF ABBREVIATIONS

JMStV – Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia	OSCE – Organization for Security and Co-operation in Europe
KJM – Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz, Germany)	OSMRA – Online Safety and Media Regulation Act 2022 (Ireland)
KoPI-G – Act on Measures for the Protection of Users of Communication Platforms, Austria	OWiG – Code of Administrative Offences (Germany)
KRRiT – Krajowa Rada Radiofonii i Telewizji (National Broadcasting Council, Poland)	PCHPR – Presidential Council of the Hungarian People's Republic
LCEN – Act 2004-575 on confidence in the digital economy (France)	PIHA – Prohibition of Incitement to Hatred Act 1989 (Ireland)
LGBTQ – Umbrella term for non-binary persons	R&D – Research and Development
LIBE – Committee on Civil Liberties, Justice and Home Affairs	RMN – Rada Mediów Narodowych (National Media Council, Poland)
NASK – Naukowa i Akademicka Sieć Komputerowa	SHA – School Harassment Act (France)
NAT – National Audiovisual Council, Romania	SKM – Systemic Conflict Management (Germany)
NetzDG – Act on Improving Law Enforcement in Social Networks (Netzwerkdurchsetzungsgesetz, Germany)	StGB – Criminal Code (Strafgesetzbuch, Austria, Germany)
NFOAPA – Non-Fatal Offences Against the Person Act 1997 (Ireland)	StPO – Code of Criminal Procedure (Germany)
NGO – Non-Governmental Organization	STUK – Styrelsen for Undervisning og Kvalitet (Danish Education and Quality Agency)
NMHH – Nemzeti Média- és Hírközlési Hatóság (National Media and Communications Authority, Hungary)	TABBY – Threat Assessment of Bullying Behaviour in Youth Online
OBPP – Olweus Bullying Prevention Program	TEU – Treaty on the European Union
ODIHR – Office for Democratic Institutions and Human Rights	TFEU – Treaty on the Functioning of the European Union
ODIHR – OSCE Office for Democratic Institutions and Human Rights	UDHR – Universal Declaration of Human Rights
OSCE – Organization for Security and Co-operation in Europe	UNHRC – United Nations Human Rights Committee
	UNICEF – United Nations International Children's Emergency Fund
	USA – United States of America
	VLOP – Very Large Online Platform
	VLOSE – Very Large Online Search Engine
	VOM – Victim-Offender Mediation (Denmark)

INTRODUCTION – IDEA, CONCEPT, STRUCTURE AND METHODOLOGY

ROLAND LINDT

*“The tongue has the power of life and death,
and those who love it will eat its fruit”*

Proverbs 18:21

The book that the Reader is currently holding is the intellectual product of two years of research conducted by the members of the Ferenc Mádl Institute of Comparative Law. Before sharing the findings of our distinguished authors, hereby we intend to summarise the ‘journey’ leading to this very point.

Since its foundation in 2019, our organisation has had the objective to engage in international scientific discourse, thus leading research in areas related to the most relevant issues discussed by European scholars of jurisprudence. In 2020, within the framework of the Department of Public Law, the decision was made to commence a major research programme in which each researcher chose a country, analysing its legal framework through a common concept. As a result, the book introducing the main concept of emergency power regulation of European countries from a comparative perspective was concluded,¹ being one of the first comprehensive works in Hungarian in this field of constitutional law, with a unique comparative approach. Little was known about the upcoming pandemic when the concept was developed. Consequently, the topic of emergency power and its limits became the centre of scientific interest on a global level. Since our work has been recognised by the Hungarian scientific society, it was soon decided to make it accessible on an international level – in 2022, a new book, this time focusing on the solutions adopted by Central and Eastern European countries, was released.²

¹ Nagy and Horváth, 2021.

² Nagy and Horváth, 2022.

Seeing the demand for further research activity with a comparative approach, discussion regarding the next major project began in autumn 2022. Based on the latest findings of our experts, both the interpretation of constitutional identity in Europe³ and legal problems of mandatory vaccination⁴ seemed promising topics. Nevertheless, we finally agreed to examine a completely new problematic area: legal reactions to hate induced unlawful activities in the digital sphere from a comparative perspective. The complexity of the subject matter required the exploration of various branches of the selected national legal systems; besides criminal law measures, we strived to recollect the most relevant rules of administrative and media regulation. During the research process, we elaborated five subtopics with a view to creating thorough country profiles: (i) regulation of hate speech; (ii) legislative and practical reactions to the phenomenon of cyberbullying; (iii) institutional measures and best practices on prevention, especially as part of education system; (iv) liability of employers – perspective of labour law; and (v) liability of online service providers. The final results were published during autumn 2023.⁵ The idea of the preparation of this current book was conceived even before the publication of our findings for several reasons. On the one hand, the comparative analysis of the country profiles⁶ revealed that national labour laws do not generally contain specific rules, but that the obligations of the employers in practice can be derived from the principles of the field in question. On the other hand, a new regulation adopted by the European Union reformed the legal framework related to platform liability in the meantime.⁷ The provisions of the regulation concerned entered into force gradually, providing sufficient preparation time for state actors and the affected legal entities; this process terminated in February 2024. Moreover, several authors referred to the fact that relevant legislative procedures were in progress in some Member States of the European Union (e.g. France,⁸ Ireland⁹ and Poland¹⁰).

In line with the above-mentioned changes, country profiles of this latest release consist of slightly different subtopics, omitting thoughts on labour law

3 For the elaboration of the issue by our researchers, see: Horváth et al., 2020; Horváth et al., 2021; Ungvári and Hojnyák, 2021.

4 For the elaboration of the issue by our researchers, see: Horváth, 2022; Horváth and Ungvári, 2023.

5 Nagy, 2023.

6 Nagy and Lindt, 2023.

7 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.

8 Szóke, 2023.

9 Horváth, 2023.

10 Benyusz, 2023.

regulation and adding a fundamental law approach in order to better enshrine the connection between the examined areas.¹¹ Furthermore, the list of the countries examined has also been modified – a chapter introducing the legal framework of the USA has not been included, instead, the summary of the Belgian regulation has become part of this work, thereby focusing exclusively on European countries.

The structure of the book can be divided into three major parts. The first part discusses general questions, including common legislative challenges emerging from technological development, approaches of the definition of cyberbullying and criminological aspects of the phenomena concerned. The second part, consisting of two chapters, one on the relevant case law of the European Court of Human Rights and one on the most important instruments of the European Union, outlines the supranational legal framework that influences the content of European national systems. Finally, the third part introduces the profiles of the selected countries, highlighting national specificities.

As regards the methodology applied, the experts, in order to identify the relevant national provisions, used the comparative approach. Here we consider necessary to explain our interpretation on this research method, since different paradigms can be recognised.¹² After World War II, the so-called functionalist approach became more and more widespread. In order to summarise the core meaning of functionalism in a nutshell, we can state that, based on the assumption that different legal systems may have significantly divergent legal notions and solutions, the followers of this trend do not strive to find almost equivalent ones, but to identify those rules that react to the same problems of society.¹³ In other words, functionalism is the problem-based approach of comparative legal research. As regulatory issues related to the digital space are relatively new, a common European doctrine with similar national notions is yet to be created. That is why the research group agreed to follow the aforementioned functionalist approach. In an effort to discover those pieces of legal norms that

11 In our opinion, the issues discussed in this book can be interpreted as practical implications of the conflict between the freedom of expression and certain fundamental rights. In this regard, a comparative constitutional analysis was also desirable, since we believe that even in Europe, legal cultures vary to an extent that the content of certain fundamental rights may differ from country to country, i.e. we applied a cultural relativistic approach of rights. On the issue of universalism and cultural relativism, see: Kovács, 2016, pp. 368–369; Bragyova, 2018, p. 25; Kardos, Lattmann and Mink, 2018, pp. 480–482. Cf. Halász, 2021.

12 For example, Hungarian scholar, *Balázs Fekete* describes three paradigms of comparative law from a historical point of view. Fekete, 2011, pp. 70–72, 109–111, 157–159. Cf. Kecskés, 2015.

13 Horváthy, 2005, pp. 10–11; Fekete, 2015, pp. 442–444. Cf. Szabó, 1975, pp. 124–127.

are regularly applied in connection with such unlawful activities, the experts also analysed works of scholars from the countries concerned and judicial practice where it was necessary.

This book contains the most important data which we have gathered over the past two years of research, supplemented by our critical insights. As these days the analysed area develops dynamically and thus new theoretical and practical challenges emerge quite often, we all sincerely hope that this base of information will serve as a useful source for further research in the field, as well as a discussion starter in the European scientific community.

January 2025

Bibliography

- Benyusz, M. (2023) 'A gyűlöletbeszéd és a kibermegfélemlítés szabályozása Lengyelországban' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet, pp. 373–395; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_14.
- Bragyova, A. (2018) 'Alapjogok – emberi jogok fogalma' in Lamm, V. (ed.) *Emberi jogi enciklopédia*. Budapest: HVG-Orac, pp. 19–25.
- Fekete, B. (2011) *A modern jogösszehasonlítás paradigmái: Kísérlet a jogösszehasonlítás történetének új értelmezésére*. Budapest: Gondolat.
- Fekete, B. (2015) 'A jogösszehasonlítás magyarországi történetének és alkalmazásának alapkérdései' in Jakab, A., Menyhárd, A. (eds.) *A jog tudománya: Tudománytörténeti és tudományelméleti írások, gyakorlati tanácsokkal*. Budapest: HVG-Orac, pp. 419–450.
- Halász, I. (2021) 'Az emberi jogok civilizációs meghatározottsága' in Bódi, S., Schweitzer, G. (eds.) *Alapjogok: Az emberi jogok alkotmányos védelme Magyarországon*. Budapest: Ludovika, pp. 19–39.
- Horváth, A. (2022) 'Mások élete? A kötelező Covid-oltások a magyar, a német és az osztrák alkotmánybírósági döntések tükrében', *Állam- és Jogtudomány*, 63(3), pp. 3–38; <https://doi.org/10.51783/ajt.2022.3.01>.
- Horváth, A. (2023) 'Új kihívások, új törvények: a gyűlöletbűncselekmények és a cyberbullying szabályozása Írországban' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet, pp. 337–372; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_13.
- Horváth, A., Pék, E., Szegedi, L., Szőke P. (2020) 'Alkotmányos identitás: pajzs, kard vagy párbeszéd? Széljegyzetek egy fogalom történetéhez I.', *Publicationes Universitatis Miskolcensis, Sectio Juridica et Politica*, 38(2), pp. 93–112; <https://doi.org/10.32978/sjp.2020.031>.
- Horváth, A., Pék, E., Szegedi, L., Szőke P. (2021) 'Alkotmányos identitás: pajzs, kard vagy párbeszéd? Széljegyzetek egy fogalom történetéhez II.', *Publicationes Universitatis Miskolcensis, Sectio Juridica et Politica*, 39(1), pp. 116–137; <https://doi.org/10.32978/sjp.2021.005>.
- Horváth, A., Ungvári Á. (2023) 'Kockázatok és mellékhatások: az olasz alkotmánybíróság döntései a kötelező Covid-oltásokról', *Pro Futuro*, 13(1), pp. 1–21; <https://doi.org/10.26521/profuturo/2023/1/13344>.
- Horváthy, B. (2005) *A jogösszehasonlítás főbb tézisei és az európai integráció* [Online]. Available at: <https://www.mek.oszk.hu/03400/03435/03435.pdf>

- Kardos, G., Lattmann, T., Mink, J. (2018) 'Univerzális és regionális emberi jogok' in Kende, T., Nagy, B., Sonnevend, P., Valki, L. (eds.) *Nemzetközi jog*. Budapest, Wolters Kluwer, pp. 477–519.
- Kecskés, L. (2015) 'A jogösszehasonlítás bővületében' in Nochta, T., Monori, G. (eds.) *Ius est ars: Ünnepi tanulmányok Visegrády Antal 65. születésnapja tiszteletére*. Pécs: Pécsi Tudományegyetem Állam- és Jogtudományi Kar, pp. 255–274.
- Kovács Péter (2016) *Nemzetközi jog*. 3rd edn. Budapest: Osiris.
- Nagy, Z. (ed.) (2023) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet; <https://doi.org/10.47079/2023.nz.gyuloletbeszed.10>.
- Nagy, Z., Horváth, A. (eds.) (2021) *A különleges jogrend és nemzeti szabályozási modelljei*. Budapest: Mádl Ferenc Intézet; <https://doi.org/10.47079/2021.nzha.kulon.4>.
- Nagy, Z., Horváth, A. (eds.) (2022) *Emergency Powers in Central and Eastern Europe: From Martial Law to COVID-19*. Budapest-Miskolc: Ferenc Mádl Institute of Comparative Law, Central European Academic Publishing; <https://doi.org/10.47079/2022.znah.epicaee.1>.
- Nagy, Z., Lindt, R. (2023) 'Összegzés – Felelősség a gyűlöletbeszédért, a zaklatásért és a megfélemlítésért a kibertérben' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet, pp. 527–555; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_20.
- Szabó, I. (1975) *A jogösszehasonlítás szocialista elmélete*. Budapest: Akadémiai Kiadó.
- Szőke, P. (2023) 'Szabadság, egyenlőség... és testvériség? A gyűlöletbeszéd és az internetes zaklatás elleni fellépés a felvilágosodás hazájában, Franciaországban' in Nagy, Z. (ed.) *Az összehasonlító jog eszközével a gyűlölet ellen – Az online gyűlöletbeszéd, zaklatás és megfélemlítés nemzetközi szabályozása*. Budapest: Mádl Ferenc Intézet, pp. 303–335; https://doi.org/10.47079/2023.nz.gyuloletbeszed.10_12.
- Ungvári, Á., Hojnyák, D. (2021) 'Gondolatok az alkotmányos identitásról a lengyel és a magyar alkotmánybíróság 2021-es határozata nyomán', *Európai Jog*, 21(6), pp. 12–16.

I. CHALLENGES OF TECHNOLOGICAL DEVELOPMENT FOR THE LEGAL DEVELOPMENT

ZOLTÁN NAGY

Hate speech and new technologies raise questions for legal regulation. To answer these questions correctly it is necessary to understand the social and technological context, in which these activities take place, and to describe the social expectations of regulation and the difficulties faced by the legislator in preventing or making it more difficult to apply the law in these specific social contexts. It is important to map the way in which technology is embedded in society and the economy in order to plan for the effects of regulation and to identify the often-inextricable threads of interdependence.

Humanity has undergone rapid biological and social evolution for the age of the Earth and, as the literature suggests, has gone from being an insignificant animal to the master of the planet over the millennia. Today, we are the only species to dominate the Earth, but during this evolution we have caused irreparable damage to the ecosystem, the effects of which we are already feeling, but the future effects of which we can only imagine.¹ Can we make use of the knowledge and opportunities that our social and economic development has given us? Will the pursuit of ever greater prosperity, technological progress and economic growth ensure a meaningful and fulfilling life for humanity. Will scientific progress offer us solutions for the future, providing answers to the problems that urgently need to be addressed. We are witnessing very rapid technological progress, the pace of which is only set to accelerate in the future. Humanity has entered a new age, the fourth age, according to the literature. The most important areas of the fourth industrial revolution are cyber-physical systems, the Internet of Things and cloud computing, data science and

¹ Harari, 2017, p. 369.

communication technologies.² The authors point out that in some eras of humanity, change has been triggered by technological advances. This development extends to all levels of life. The effects of artificial intelligence and robotics are less felt today, but the impact of network science, the internet and computing on social and economic development is clear.³ The way people communicate, and transfer data has undergone a sea change.⁴

Innovation and technological progress have been an important condition for social and economic development. Economic growth is influenced by many factors, and four main drivers have been identified in the economic literature: human resources, natural resources, capital and technology. The four elements are important, but economic history shows that technological progress has resulted in large part from rising output, productivity and living standards.⁵ The technological aspect of economic growth is highlighted by the growth of the information economy. The literature suggests that this may be a function of two factors, automation and the use of managed information, the explosive development of databases and communication networks.⁶

However, technological progress requires more than just science; it also requires the active role of the state and the economy in providing the resources for technological progress and in applying technological advances.⁷ The importance of this is that, according to economic experts, only technological progress can ensure a steadily rising standard of living and economic growth.⁸ It will therefore become essential in the future to understand its economic and social importance. This is particularly important given that technology has two important characteristics: it is a non-competitive good and it is not excludable. Technology can be used by several people in parallel, in simultaneous activities, it is usually not in physical form, it can be used infinitely many times and is therefore not a competing good. On the other hand, the lack of excludability is an important feature, as the limited possibilities associated with it may reduce the gains from the technology, as it is difficult to exclude unauthorised users from exploiting the technology. Thus, the role of the state in relation to technological development in general is enhanced. The state intervenes in the market through financial and private regulation to promote R&D. It promotes technological development through direct and indirect subsidies

² Fülep, Nick and Várgedő, 2018, pp. 45–46.

³ Reese, 2020, pp. 259–266.

⁴ Bell, 2001, p. 23.

⁵ Samuelson and Nordhaus, 2012, pp. 475–480.

⁶ Bell, 2001, p. 16.

⁷ Harari, 2017, pp. 227–230.

⁸ Mankiw, 2005, pp. 133–136.

(tax preferences) and addresses the problem of foreclosure by protecting intellectual property, i.e. by creating the possibility that only the inventor owns the technological innovation. These instruments facilitate R&D activities by ensuring that the development pays off and generates profits. Without all these incentives, technological progress would be slowed down and jeopardised.⁹ At the same time, modern digital infrastructure is not owned by the state but by private companies, i.e. social media platforms, the framework for the digital public sphere.¹⁰

However, the extent to which a society can adapt to new technology is also important. If this is successful, technology will be an important factor in economic and social transformation. But the benefits are significant if this adoption happens quickly. However, a key prerequisite for this is legislation, human resources, adequate funding and close cooperation between different sectors.¹¹

Technology therefore has an impact on the economy, but also on society, and these also have an impact on technological development. Social and technological developments may be different, but they can also evolve together. Technology is characterised by its social construction, i.e. it is created by people and used by people, so there is an interactive relationship between technological development and social development. It is the transfer of technology that makes a given development a market product, but it is the economic and social environment that makes its diffusion possible. It is very important, however, that technologies are adaptable to the social situation, otherwise their development will stop, and others will take their place.¹² However, social science research also shows that society and technology are not separate entities but interact closely. The relationship between the objects created by technology and their users takes on a specific shape as technology develops. New relationships and interrelationships are emerging between people and the tools created by new technology. A profound change in social relations is taking place, and the relationship between objects and people is becoming more deeply intertwined. The nature of objects is changing, but the social relations of people are also changing. According to the literature, there is a tangible process on the tool side. Objects exist in real and digital space, they have a strong communicative potential, they are increasingly intelligent, they are characterised by a higher level of autonomy and they are strongly embedded in society. Large multinational

⁹ Mishkin, 2015, pp. 222–226.

¹⁰ Balkin, 2018a, pp. 989–990.

¹¹ Holczer, 2007, pp. 92–98.

¹² Kincsei, 2007, pp. 48–62.

media platforms are located between the state and the people. In this new algorithmic society, communication depends on the decisions of the owners of the private infrastructure, who control the digital space, i.e. the problem of private governance arises. These private companies control, censor and monitor communication on the platforms.¹³

In examining the human side, the literature highlights that humans have become vulnerable to technology, their personalities are split into real and virtual personalities, in many cases becoming monitored, controlled and controlled personalities. Human relations are mediated by objects, self-expression takes place through objects and, as part of networks, the information communicated can be deformed, its mechanism of action becoming uncontrollable and unmanageable.¹⁴ New media applications are both a method of communication and a method of observation. They provide increasingly accurate ways of monitoring the behaviour of end-users and those who communicate with them. In what is seen in the literature as the great bargain of the twenty-first century, social media providers offer valuable services for free, in return for which they can collect, analyse and use end-user data to control users, and all this under digital privacy.¹⁵

The relationship between technological devices and people is defined in the literature by several theses. The first is that the impact of technology goes beyond its use and utility. A further important thesis is that the device is in relationship and interaction with the user. Technology also satisfies the desire for something different, for something newer, since tools are typically incomplete, evolving and offering the user future versions. This desire for newer devices also sustains the system of production and technological innovation and newer technology generates new demand from the user. Current development trends suggest that the technological world and human relations are becoming increasingly intertwined and complex.¹⁶ The literature explicitly refers to the fact that we live in an information society, which is a new way of living together in society. Not only are technological innovations emerging, but social coexistence (habits, norms, culture) is changing as a consequence. The basis for these changes is made possible by information and communication technology. Networking is promoting globalisation and creating a global information society among those who participate in the network.¹⁷

¹³ Balkin, 2018b, pp. 1150–1154.

¹⁴ Csizmadia, 2019, pp. 63–68.

¹⁵ Balkin, 2018a, pp. 991–994.

¹⁶ Csizmadia, 2019, pp. 62–63.

¹⁷ Pintér, 2007, pp. 21–26.

The information society¹⁸ is transforming the world, with globalisation, networking and a global media culture being among its many important features.¹⁹ The relationship between physical space and time is changing, with technology making it possible to bridge the physical space in the flow of information in a very short time. This will also help to reduce inequalities between spaces. Channels of globalisation and interconnectivity are emerging through the Internet, which strengthens social links and networks society. The Internet is strengthening network industries and multinational companies that respond to and serve social demand. A global digital economy has been built through technology that serves consumer needs at an increasingly higher level, which also encourages these companies to develop technology rapidly.²⁰

In order to address the issues of legal regulation, it is necessary to understand the problems that arise in the context of the information society. The literature raises a number of these issues, of which I will highlight those that are relevant from a legal point of view. One issue is the level of organisation of the supranational level, the global information society. Other important issues are data protection and information security, the relationship between government and citizens, and future developments that will induce further changes (artificial intelligence, robots).²¹ It is therefore important how law responds to these issues.²² There is a literature that stresses the importance of the relationship between technology and law in terms of the problems that technology brings

18 Pintér, 2007b, pp. 213–246. The author points out that the concept of information society can be approached from different angles, and different concepts can be given depending on the perspective from which the concept is approached. In the technological sense, it refers to operations with information and knowledge and the associated infocommunication tools; in the social sense, it is characterised by a network society, communality, continuous adaptation, new forms of inequality and globalisation; in the development sense, it refers to a paradigm shift and a way of thinking; it can also be defined as an object of scientific study.

19 Zódi, 2018, pp. 36–39.

20 Kollányi, 2007, pp. 83–92.

21 Z. Karvalics, 2007, pp. 44–46. The author breaks down the issues of the information society into nine main areas. These areas are the global information society, sustainable information society (environmental problems), information society security (technology-related risks), space-oriented information society (impact of space exploration), electronic Orwellian world or digital Athens (new kind of dictatorship or new kind of democracy), smart city, corpus digitale (preservation of all human knowledge), creative information society, post-information society (future development).

22 Manwaring, 2017, p. 62. Among the innovation issues, the author highlights the variability and vulnerability of computing, the interaction between the physical world and cyberspace, the impact of digital objects and devices, electromobility, the relationship between humans and computers, the impact of autonomous and semi-autonomous devices.

to the forefront of social life that did not exist or were not relevant before. In many cases, the challenge for legal regulation is not the technology itself, but the way technology is used. Technology also means social relations between people, which are in a state of constant change, and therefore the problems associated with the development and use of technology are changing rapidly. People interact with technology and with each other. Technology thus triggers innovation in social and legal relations. Technology enters into an existing social and legal system and challenges and changes the traditional regulatory system, disrupting the functioning of traditional legal institutions, and requiring new responses to challenges.²³ A particularly important factor is the issue of technological governance, where modern technologies are often used as a regulatory tool instead of legal rules. Through technology governance, certain actions or people are excluded from technologically regulated activities by automating processes. However, this techno-regulation raises many problems, for example, it may violate legal freedoms. At the same time, technologies are also generally considered in the literature to have a disruptive effect, as they disrupt the existing regulatory order.²⁴

The theory also seeks answers to the questions raised. The literature divides theories on information society governance into three groups. One of these is the question of jurisdiction. The example of the Internet shows that in some cases no single state has exclusive jurisdiction over a given technology. This view emphasised that, without state intervention (e.g. the Internet), users themselves shape the rules of operation, the ethical rules. However, self-regulation is inadequate to address the problems at hand. The use of technology was not separate from the existing social reality and therefore could not be treated as a 'rights-free space'. Existing social norms must be taken into account, the relevant legal regulation of which already exists. The other view is that technology is a specific subject of regulation and that, accordingly, a completely new regulation needs to be developed. Thirdly, the theory of integrated regulation has been developed and put into practice. In other words, it is not necessary to develop a completely new regulatory framework, but rather to extend the existing regulatory framework to the new technology. This does not mean that new concepts do not need to be created, but that the legal instruments are available and can largely be applied to the social conditions changed by technology.²⁵

Ex ante and *ex post* regulation is an important issue in relation to legal regulation. The literature emphasises that *ex ante* regulation is difficult in the case of

23 Balkin, 2015, pp. 46–55.

24 Brownsword, 2015, pp. 1–51.

25 Simon, 2007, pp. 114–118.

technology, since it is a new regulatory area and there are unknown situations to be considered. Excessive *ex ante* regulation can hamper technological development and lead to poor solutions. *Ex post* regulation allows the legislator to know the subject matter of the regulation and the life situations to be regulated and to intervene only where and to the extent necessary.²⁶ However, too late regulation carries the risk that the legislator loses control of the technology and may create confusion in the application of the law.²⁷

The law also must face up to a number of specificities arising from the nature of the technology which may give rise to regulatory anomalies. One such problem is the issue of regulatory gaps, where uncertainty about technology can lead, for example, to the emergence of a relatively new, unknown technology and where even science cannot precisely define and describe the technology. The other area is connected to the problems regarding the application of existing regulation. A major challenge before the law in force is to integrate new areas of regulation into the current regulatory environment. If the law captures and describes the technology incorrectly, the regulation will be incorrect and imprecise. Another problem is the scope, impact and use of technology. Furthermore, deviations from the model predicted and assumed by the law can also cause confusion in the regulatory environment. The issue of over- or under-regulation may also arise. Both can be a problem in the economic and social functioning and interaction of technology. Finally, it is important to highlight the rapid regulatory obsolescence. The law changes slower than technology and the social and economic conditions that it creates.²⁸

It is therefore clear that there is a conflict between law and technological progress. One of the main problems with technology is uncertainty. How will the novelty affect social relations, what will be the result of this and its application, how will social relations affect the technology itself? Law tries to manage these risks, to protect human rights against technology. This may even lead to the law restricting the use of the technology until it is proven that it is safe and conforms to the prior norms set by the law. The dilemma therefore arises of whether to regulate quickly but less optimally, or to regulate slowly but judiciously, waiting for social and economic conditions to evolve.²⁹

The literature also points out that for a time, the traditional instruments of law were able to keep pace with technological change by incorporating and supplementing the emerging regulatory issues into the traditional regulatory

²⁶ Simon, 2007, p. 115.

²⁷ Nagy, 2018, p. 38.

²⁸ Butenko and Larouche, 2015, pp. 66–68.

²⁹ Tóth-Klein, 2018, pp. 30–32.

system. However, in recent decades, further problems have emerged. One of these problems is the diffusion of technology. With the spread of information technology, much more profound changes are taking place than experts thought in the early years of its diffusion. And qualitative changes have forced law to intervene in social relations in a stronger way. This can take place at two levels: the legislature and the application of the law. Of these two, it is the application of the law that is likely to be slower to adapt, since it is here that changes in the traditional application of the law are needed, even generating differences in perception between generations of jurists.³⁰

The literature breaks down the problematic field for law based on technology into three main areas. Platforms, robots and artificial intelligence, and Big Data. Horizontal and vertical platforms, which become ‘online living spaces’, act as a kind of ‘digital utility’.³¹ The characteristics of the Internet have a fundamental impact on the potential for legal problems to arise. These include openness, multimodality, interactivity, digital nature, convergence, decentralisation, globalisation, anonymity, lack of control and continuous technological development. The Internet is an open network to which anyone can connect, and which allows the downloading and transmission of multimedia content. At the same time, it is also a digital repository for content, thus increasingly integrating multimedia, communication and computing. It is also a decentralised network that can operate without control, spanning the whole world and providing a degree of anonymity for the user.³² However, it also seems that platforms are forced to self-regulate and censor themselves because of corporate responsibility and economic reasons. The platforms moderate hate content and allow users to filter unwanted content, showing corporate responsibility towards users and at the same time limiting full freedom of expression. But in addition to the noble objective, there is another reason why platforms are influenced, and that is economic. If users are turned off by hateful, violent content, this threatens advertising revenue and the profits that could be made from it. If the platform better meets

³⁰ Zódi, 2017.

³¹ Zódi, 2017, p. 28. In the other cited work, the author clarifies the issue of horizontal and vertical platforms (Zódi, 2018, pp. 101–103 and pp. 165–167). By horizontal platforms he means websites that connect people and other resources through algorithm-driven data flows and that have a sufficiently large number of users connected to them to measure their social impact (e.g. Google, Facebook). Vertical platforms are understood as enterprises that enable value-creating interactions, facilitate economic activity, act as a kind of virtual marketplace (sharing economy, e.g. UBER).

³² Nagy, 2004, pp. 58–61. The author points out that anonymity is apparently present because the computer logs our searches, and service providers also collect data about the user and the computer can be used to trace the user.

users' needs and preferences, then users will visit more regularly and there will be more advertising opportunities. A balance must therefore be found between ensuring freedom of expression and hate content. In this sense, platforms play the leading role.³³ A commitment to digital citizenship requires ensuring robust and responsible participation in the online space. However, the proliferation of hate speech requires more complex solutions. The literature highlights three such areas, such as removing hate content; countering hate speech with counter speech; online dialogue and the education of users. The first solution is considered the most effective, but also the most powerful tool, by blocking the content or terminating the user account. In the second case, a milder tool is used, i.e. creating a dialogue, refuting the comments. Thirdly, as a means of education, platforms can inform users about the standards they apply, the content they remove and the reasons for their removal.³⁴

All these legal issues are also of great relevance to our book. Jurisdiction, competition, fundamental rights and data protection issues arise in the case of horizontal platforms. In the area of jurisdiction, the question arises: how national regulation can regulate activity in a global, non-national, transnational space? National regulators are ineffective or have little or no influence in this area. Competition issues arise because of the small number of market operators. The specificity of the network industry itself results in a monopoly of service providers, with users flowing to one provider as a self-expanding process. However, the 'monopoly situation' is not limited to one country but extends to the whole world. This situation is exploited by operators from economic and other points of view. The question arises whether the service provider only gives the customers the possibility to do and post anything they want on the internet or whether they have to control the content. Where is the limit and under what law does the service provider do this, can the content be checked under the internal rules applicable to a private company? The literature also points to the important regulatory and legal interpretation issues that emerge in this area. A platform-related issue is digital data storage and use. This is also a fundamental rights issue, which falls under data protection.³⁵

There are also significant legal dilemmas in the other two areas. Vertical platforms operate as a business model, a kind of 'virtual marketplace'. The sharing economy³⁶ is a service sector using innovative digital solutions, which causes problems in several legal areas such as competition law (violation of industry

³³ Klonick, 2018, pp. 620–629.

³⁴ Citron and Norton, 2011, pp. 1471–1491.

³⁵ Zódi, 2017, pp. 27–29.

³⁶ Nagy, 2016, pp. 1–7.

rules), consumer protection (exclusion of liability), labour law (forced employment, hidden employment contracts), tax law (tax avoidance), among others.

A more complex issue is artificial intelligence and robots. Even in jurisprudence, there are divergent views on the provision and legal recognition of electronic identity. Is it an autonomous entity that makes autonomous decisions or is it just a programmed object that carries out the programmer's commands? Several questions arise in relation to damages and compulsory liability insurance.³⁷

The European Union is also looking for answers to technological challenges, which need to be addressed through legislation. In addition to defining four main strands, economy, infrastructure, governance and expertise, digital citizenship is at the heart of the question of rights and principles for digital development. These principles will be translated into rights and become part of national legislation. These principles include people-centredness, freedom of choice, safety and security, maintainability, participation, solidarity and inclusiveness. Protecting the rights of individuals, a fair online environment, protection against illegal and harmful content, and ensuring the security of the digital environment are therefore important issues. Internet access for all, digital infrastructure and digital public services are priorities. Many of the digital rights are not new rights but complement existing rights.³⁸ EU legislation has developed along these lines, through the Digital Service Act (DSA) and the Digital Markets Act (DMA). The DSA is seen by the EU as platform regulation, as the previous rules were outdated and not suited to deal with modern changes. This regulatory crisis has been resolved by the new regulation.³⁹ Indeed, the EU has also acted as a model regulator to address the regulation of artificial intelligence. At the time of writing, this has not yet been adopted, but it is a forward-looking initiative in many respects. The European Union has set a fundamental objective to ensure that the reliable, safe development and use of AI is carried out in accordance with fundamental rights, and that innovation is accompanied by human-centred technology.

This brief overview shows that law is constantly facing new challenges as technology changes, and the number of challenges will only increase in the coming decades. Members of society see only the great freedom and the expanding digital space and opportunities offered by technology and are not alert to the

37 Zódi, 2018, pp. 28–71.

38 *Europe's Digital Decade: digital targets for 2030* [Online]. Available at: https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/europes-digital-decade-digital-targets-2030_hu.

39 Zódi, 2023, pp. 181–201.

dangers inherent in this. When infringements occur, however, people immediately expect the state to provide legal protection, even though they may have previously refused to legislate in this area. The use of technology does not improve basic human qualities or human relationships, but only transfers them into a digital space. The law is constantly shaping the rules in response to problems, but there is clearly an inherent slowness of reaction time in lawmaking that cannot be eliminated if the legislator is to act in spirit of democratic norms and prudence. In comparison, service providers can change internal rules more quickly, even on the basis of external government regulation – but is this the right practice? However, in my opinion, the task of incomplete regulation cannot be left entirely to the service provider. It would be better to develop a more flexible legal regulatory regime involving providers who are more familiar with the technology. In any case, these are challenges that both practitioners and academics need to be prepared for.

Bibliography

- Balkin, J. M. (2015) 'The Path of Robotics Law', *California Law Review Circuit*, 2015/6, pp. 45–60.
- Balkin, J. M. (2018a) 'The First Amendment in the Second Gilded Age', *Buffalo Law Review*, 66(5), pp. 979–1013.
- Balkin, J. M. (2018b) 'Free Speech in the Algorithmic Society: big data, private governance, and new school speech regulation', *U.C. Davis Law Review*, 51(3), pp. 1149–1210; <https://doi.org/10.2139/ssrn.3038939>.
- Bell, D. (2001) 'The social framework of the information society', *Information Society*, 1(1), pp. 3–33.
- Brownsword, R. (2015) 'In the Year 2061: From Law to Technical Management', *Law, Innovation and Technology*, 7(1), pp. 1–51; <https://doi.org/10.1080/17579961.2015.1052642>.
- Butenko, A., Larouche, P. (2015) 'Regulation for innovativeness or regulation of innovation', *Law, Innovation and Technology*, 7(1), pp. 52–82; <https://doi.org/10.1080/17579961.2015.1052643>.
- Citron, D. K., Norton, H. (2011) 'Intermediaries and Hate Speech: Fostering Digital Citizenship for Our Information Age', *Boston University Law Review*, 91(4), pp. 1435–1484.
- Csizmadia, Z. (2019) Az autonóm, önvezető technológiák elterjedésének társadalmi következményei – kérdések, dilemmák és szempontok', *Tér – Gazdaság – Ember*, 6(1), pp. 59–85.
- Fülep, I., Nick, G., Várgedő, T. (2018) 'Zászlón a digitalizáció – Ipar 4.0', *Új Magyar Közigazgatás*, 11(2), pp. 45–55.
- Harari, Y. N. (2017) *Sapiens – Az emberiség rövid története*. 2nd edn. Budapest: Animus.
- Holczer, M. (2007) 'Innovációs verseny az információs társadalomban' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 94–113.
- Kincsei, A. (2007) 'Technológia és társadalom az információ korában' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 47–63.
- Klonick, K. 'The New Governors – The People, Rules, and Process Governing Online Speech', *Harvard Law Review*, 131(6), pp. 1598–1670.
- Mankiw, N. G. (2005) *Makroökonómia*. Budapest: Osiris.
- Manwaring, K. (2017) 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies', *Deakin Law Review*, 22(1), pp. 53–84; <https://doi.org/10.21153/dlr2017vol22no1art722>.
- Mishkin, F. S. (2015) *Makroökonómia*. Budapest: Alinea.

- Nagy, D. (2004) 'Az internet és a jog', *Információs Társadalom* 1.sz, pp. 58–68; <https://doi.org/10.22503/inftars.IV.2004.1.4>.
- Nagy, Z. (2016) 'A közösségi gazdaság (Sharing Economy) és pénzügyi szabályozása' in Kékesi Tamás (szerk.) *The Publicationes of the MultiScience – XXX. microCAD International Multidisciplinary Scientific Conference*. Miskolc: University of Miskolc, pp. 1–7; <https://doi.org/10.26649/musci.2016.121>.
- Nagy, Z. A. (2018) 'A jövő tegnap óta tart- A modern Technikai-technológiai folyamatok kihívásai a jog területén', *Belügyi Szemle*, 66(10), pp. 36–55; <https://doi.org/10.38146/BSZ.2018.10.3>.
- Pintér, R. (2007a) 'Úton az információs társadalom megismerése felé' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 11–28.
- Pintér, R. (2007b) 'Divatos hívószavak, nagy elméletek, fejlesztési szupernarratívák és metanarratívák – Az információs társadalom jelentésvilága' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 212–223.
- Reese, B. (2020) *A negyedik kor – Okos robotok, tudatos számítógépek és az emberiség jövője*. Budapest: Typotex.
- Samuelson, P. A., Nordhaus, W. D. (2012) *Közgazdaságtan*. Budapest: Akadémiai Kiadó.
- Simon, É. (2007) 'Bevezetés az információs társadalom jogi szabályozásába' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 114–129.
- Tóth, A, Klein, T. (2018) 'Technológia és robotjog' in Tóth, A. (szerk.) *Az infokommunikációs és technológiai jog alapjai*. Budapest: NKE, pp. 30–45.
- Z. Karvalics, L. (2007) 'Információs társadalom-mi az? Egy kifejezés jelentése, története és fogalomkörnyezete' in Pintér, R. (szerk.) *Az információs társadalom*. Budapest: Gondolat-Új Mandátum, pp. 29–46.
- Zódi, Zs. (2018) *Platformok, robotok és a jog*. Budapest: Gondolat Kiadó
- Zódi, Zs. (2017) 'Az információs társadalom legújabb kihívásai a jog számára', *Gazdaság és Jog*, 2017/9, pp. 27–30.
- Zódi, Zs. (2023) *Platformjog*. Budapest: Ludovika.

II. IN THE GRIP OF A CHANGING WORLD – CONCEPTUAL AND FORMAL APPROACHES

—— LÁSZLÓ DORNFELD – ERIKA VÁRADI-CSEMA ——

It is essential for the topic of this book to define what exactly is meant by *cyberbullying*, as the lack of a proper conceptual framework is detrimental to the understanding of the topic.¹

The diversity and differences of concepts and content is due to a number of reasons. The phenomenon is complex and cross-disciplinary. Highlighting other elements is important for the psychologist, the pedagogist, the criminologist or even the criminal lawyer. The fact that the constant development of information and communication technologies is helping to give rise to new forms of activity that are not yet known is also a challenge for professionals. The other fact, that as many of the consequences of the phenomenon, particularly in the long term, are not sufficiently understood or have not been researched. The rapid development of research methods in fields such as neuroscience and medical technology is also an important factor to deeply understand the phenomenon. It is not only the external conditions that are changing, but also the victims of abuse. For example, with the arrival of new generations, the low degree of digital resilience and the high level of mental and emotional vulnerability is a relevant issue, while for older generations, who are increasingly active in the online space, it is the increased degree of victimization that is more important.

In this changing world, there is a need to develop a conceptual framework that can cover all legally relevant aspects of the phenomenon under consideration, while ensuring an adequate criminal law response.

¹ Pongó, 2021, p. 34.

1. Conceptual diversity: from bullying to cyberbullying

The English-language term is often used in other languages to fill in the missing concept, although it is not uniform (in Germany and the Scandinavian countries, for example, *cybermobbing*, which is also of English origin, is the common term).² There are also examples of cyberbullying being identified with *online harassment*³ although the two terms are not synonymous. Criminal harassment and cyberbullying are two distinct categories, but there is a very narrow intersection between the two, whereby electronic bullying also constitutes the crime of harassment.⁴ In contrast, in the domestic literature e.g., the more expressive *online* or *cyber-intimidation* is gaining ground and has been adopted at the official level, for example in the Digital Child Protection Strategy of Hungary.⁵

According to Katalin Parti, the conceptual elements of bullying are:⁶

- (a) physical, verbal or psychological assault or intimidation intended to cause fear, distress or other harm;
- (b) power imbalance (physical or psychological), exploited by the stronger person (or persons) to exert pressure on the weaker;
- (c) a regularly recurring or prolonged situation between two or more people.

The most widely accepted conceptual definition of bullying comes from a 1997 article by Dan Olweus,⁷ which is at the core of attempts to conceptualize cyberbullying. He defines bullying as when a student is subjected to repeated and prolonged negative actions by one or more students.⁸

Compared to this original definition from 1997, the content of bullying has also changed. Gabriella Kulcsár analyses this development in detail in her monograph⁹. The range of defining elements is partly different for each definition: while the original 1997 concept emphasizes the repetitive nature of harassment, in addition to intentionality and the lack of balance of power, the newer definitions define a more detailed set of criteria.

² Nocentini et al., 2010, p. 130.

³ See, for example, the UNICEF information page in Hungarian. <https://unicef.hu/cyberbullying>

⁴ Monori, 2016, p. 247.

⁵ The Digital Child Protection Strategy of Hungary, p. 22.

⁶ Parti, 2016, p. 115.

⁷ The study was translated by Éva Dudik and published in Hungarian. Olweus, 1999, pp. 717–739.

⁸ Olweus, 1999, p. 717.

⁹ Kulcsár, 2024, p. pp. 43–54.

It is worth noting that the scientific approach of almost the same professional community can change – even within a short period of time. A good example of this is the definition developed in 2021 and 2023 by the working group set up by UNESCO and the World Antibullying Forum.

The 2021 concept emphasizes the role of the education system and school standards. The same set of actors ('between students'), the occurrence of physical, emotional and peer harm, the existence of a power imbalance, and the interpersonal and online format are important. However, there are no essential criteria such as intentionality or repetitive nature of the act.

In comparison, the current recent approach – next to the maintaining the social nature of the process, the occurrence of physical, emotional, peer harm, the importance of peer and institutional norms and the power imbalance – contains a number of differences. It identifies the repetition (or the risk of repetition) and intentionality as renewed criteria. At the same time, it includes adults as well as students, does not specify the specific form of bullying, but allows for the abuse to be at the level of the individual, the group or the community. This conceptual flexibility is illustrated by the extent to which the views of the same professional community can change in just some years.

As with bullying, there are different approaches to the concept of cyberbullying¹⁰ – depending on whether the focus is on the psychological, criminological or legal aspects of the phenomenon. For example, the psychological elements played an important role in an earlier concept from 2008: *"Cyberbullying is an aggressive, intentional act carried out by a group or individual, using electronic forms of contact, repeatedly and over time against a victim who cannot easily defend him or herself."*¹¹ In contrast, an approach from 2023 focuses more on the criminological aspects: *"Cyberbullying is willful and repeated harm inflicted through the use of computers, cell phones and other electronic devices."*¹²

It is not only the interdisciplinary difference in approach that is reflected in the different definitions. There is also a debate among researchers on the question of whether cyberbullying is a separate act or just a simple form of bullying in the online space. Olweus himself takes the latter view, while others argue that the particularities of cyberspace (e.g. the preservation of anonymity) require a different kind of response.¹³

There are a number of common elements between the various concepts of cyberbullying, which can be identified in most definitions. These are:

¹⁰ For more details, see Pongó, 2021, pp 30–62.

¹¹ Smith, 2014, p. 18.

¹² Hinduja et al., 2024, p. 10.

¹³ Parti, 2016, p. 116.

- (a) (intentional) harm,
- (b) repetition over time, and
- (c) power imbalance between the victim and the perpetrator(s).

However, recent research shows that these do not always appear so clearly in practice. For example, repetition raises the question of whether it is feasible on the Internet with a single content sharing?¹⁴ After all, the negative (defamatory, abusive) content posted remains accessible, shareable and transmissible in the online space. Thus, a single act of cyberbullying can lead to ongoing victimization.¹⁴ The important question is whether it is considered repetitive if this content, once shared, is subsequently interacted with (spread, shared, etc.) again and again. In my view, such cases can also be considered repetitive and thus meet the conceptual criterion of cyberbullying.¹⁵

Anonymity may be an important element, which may be one of the manifestations of the imbalance of power in cyberbullying,¹⁶ as the perpetrator may conceal his/her identity from the victim, or even the bullying itself may take place in a space from which the victim is barred (e.g. in a secret online group); thus, while he/she becomes the target, nothing will be known about the perpetrator. It should be added that there are also forms of bullying in schools where the perpetrator may remain unknown to the victim (e.g. spreading malicious rumors).

In any case, it is worth mentioning that Tamás Pongó, drawing on American examples, captures the essence of the term in his book: “*an intentional, single or repeated behavior by an electronic device that causes harm or injury to the victim, with the aim of upsetting the balance of power between the perpetrator and the victim*”.¹⁷ It is a step forward, because his concept has elements which are important also from the criminal legal field.

Based on the above, we can establish the following as the conceptual criteria for cyberbullying:

- (a) an attack of some kind intended to intimidate the victim
- (b) it takes place in the online space using an electronic device
- (c) single or repeated conduct
- (d) power imbalance.

¹⁴ Nocentini et al., 2010, p. 131; Parti, 2016, p. 116.

¹⁵ Schenk, 2020, p. 277.

¹⁶ Parti, 2016, p. 116.

¹⁷ Pongó, 2021, p. 34.

In terms of perpetration, the information and communication technologies used include instant messaging services (e.g. Viber, WhatsApp, Skype), chat applications (e.g. Messenger, Snapchat), social media sites (e.g. Tiktok, Facebook, Instagram), video sharing sites (e.g. YouTube), email, blogs, forums, websites, some of which are specifically designed to defame others, but cyberbullying can also be committed on mobile phones or even in online role-playing games. Among students, such abusive behavior is most often carried out through instant messaging.¹⁸

In order to clarify the content of the concept, a number of documents also identify possible concrete forms of cyberbullying. For example, the Digital Child Protection Strategy of Hungary classifies the following types of behavior as cyberbullying:¹⁹

- (a) *flaming*: deliberate provocation of online fights, offensive comments;
- (b) harassment;
- (c) defamation: the publication or sharing of vicious rumors that are likely to damage reputation;
- (d) ostracism;
- (e) outing: sharing secrets, rumors or other personal information with others without permission;
- (f) *trickery*: obtaining personal information from someone by fraud or deception and then sharing that information with the community;
- (g) *cyberstalking* (online surveillance): monitoring and offensive circumvention of the victim's online habits, sending threatening, intimidating messages and using them to create fear to make the other person feel that their safety is at risk;
- (h) online threats: direct threats or disturbing statements that appear to make the author appear emotionally disturbed and contemplating harming someone else or himself/herself or committing suicide;
- (i) sexting: a contraction of the word 'text' and the word 'sex', it refers to the sending of naked pictures of oneself. Although some sources, such as the Digital Child Protection Strategy of Hungary, only provide so much information on the content of sexting, it is worth adding that cyberbullying actually occurs when the images sent during sexting cause the sender to be a victim of abuse/abuse, e.g. by further unauthorized sharing of the images, etc.).

¹⁸ Preuß, 2019, p. 98.

¹⁹ The Digital Child Protection Strategy of Hungary, pp. 22–23.

2. Criminological aspects of the use of the term

The phenomenon, which primarily but not exclusively concerns young people, also gained attention in the *criminological literature*²⁰, where several terms are used, some of them synonymously. In terms of content, *bullying* is a form of aggressive behavior of a repetitive nature directed against a person who, for whatever reason, is unable to defend himself or herself (for example, someone who is physically weak). Similar behaviors are covered by *mobbing*, which means assault and is used primarily to cover the phenomenon of harassment or psychological terror in the workplace. *School violence* covers verbal, psychological, physical and sexual abuse between different groups of people (students, teachers, parents). The essential element of *school bullying* is the repetitive, prolonged nature of the aggressive act, which may happen in the form of an active, public action against the victim (direct bullying) or through ‘mere’ ostracism (indirect bullying). Where there is no objective obstacle (e.g. physical violence), all of the above types can be committed by means of modern communication tools, using *cyberspace*.

In addition to the concept of cyberbullying, there are several sources²¹ which prefer the term *cyberaggression*. According to experts, the term primarily covers the phenomenon of aggression on ICT platforms, whose targets may be specific groups, individuals, celebrities or even randomly selected victims. While cyber-harassment is defined partly as an imbalance of power and partly as repetitive, cyberaggression is defined as a form of harassment with a specific intent. In their view, the general characteristics of bullying behavior on social media are closer to this concept than to cyber-harassment or cyberbullying. Some argue²² that the strict criteria mean that phenomena such as ‘happy slapping’ should be excluded, while they can be classified under the conceptual umbrella of cyberaggression, defined as a form of social aggression. Other experts, such as Gabriella Kulcsár²³, are of the opinion that there is no missing criterion, since the possibility of repetition exists here too – albeit not directly, with new attacks on the victim, but indirectly, through the widespread display and replayability of the recording, which is a result of its shareability.

It is also important to note that for young people, as shown by a study²⁴ covering several EU countries, repetition was less important as a defining element

20 See e.g. Csemáné Váradi, 2019, 2021.

21 See, for example, Nakano – Suda – Okaie – Moore, 2016. But this definition is also used, for example, by Antipina – Bakhvalova – Miklyaeva, 2020, pp. 402–414.

22 Corcoran – Mc Guckin – Prentice, 2015, p. 252.

23 Kulcsár, 2024, p. 47.

24 Menesini et al., 2012, pp. 455–463.

of cyberbullying than power imbalance, intentionality and anonymity. This is due to the recognition that offensive content can spread in virtual space without the perpetrator's involvement in a 'viral' way, due to the use of information and communication tools – i.e. repetition is not related to the perpetrator's activity.

Another effect of this technology is that it can 'victimize' a large number of people who cannot be identified in advance.

Intentionality, i.e. the intention to abuse, is another important factor for young people in deciding how to evaluate the behavior of the other party. In the absence of the element of intentional harm the perpetrator's behavior is seen as 'just' a bad joke or crude humor.²⁵

Anonymity is an equally important factor. The very fact of anonymity tends to make the behavior more serious for the victim; however, if there is no presumption of intentionality, anonymity is less likely to be identified as cyberbullying.

According to the respondents, the most striking feature of the phenomenon is the imbalance of power.²⁶ The relevance of this criterion was prominent in all countries and in all types of behavior, and was more important than the fact of the intent to abuse. The psychological mechanism of the phenomenon, precisely because of the characteristics of the online space, is capable of greatly magnifying the victim's sense of defenselessness and, therefore, helplessness. The perception of vulnerability on the Internet on the victims' side might completely independent of the existence of the actual physical, psychological, social, etc., dominance of the attacker. Due to the way ICT tools work, preventing hurtful, harassing behavior or its 'material' manifestation from reaching others is typically not possible, or only to a limited extent with the help of a professionals, and the perpetrator's power is therefore multiplied, even in the case of less severe forms of behavior. This is partly why (offline) bullies in a face-to-face context are described as more popular, smarter and stronger than their online 'peers'.

3. Hate speech and cyberbullying

The concept of hate speech needs to be specifically mentioned for the phenomenon under consideration in this book. The term itself, as a separate category, is in fact a type of online communication with a hostile attitude, aimed at insulting the honor of a person, persons or social groups, and at degrading the community.

²⁵ Nocentini et al., 2010, p. 137.

²⁶ Menesini et al., 2012, p. 459.

A more detailed definition is given, for example, by Cohen-Almagor,²⁷ who explains that hate speech is any bias-motivated, malicious speech directed at a person or group of people because of some of their perceived or real characteristics. An important characteristic is that it expresses discriminatory, intimidating, disapproving, hostile and/or prejudicial attitudes towards characteristics of the targeted group such as gender, race, religion, ethnicity, nationality, skin color, disability or sexual orientation. Hate speech is intended to insult, dehumanize, harass, intimidate, degrade, humiliate and victimize its targets as well as incite insensitivity and brutality towards them.

Hate speech can take many different²⁸ forms, and thus, we can also find different definitions. Despite the diversity and the different focal points, the essential common element of the concepts is the insulting or belittling of the target group or its members, through the denigration of the defining characteristic of the person or group of persons. In practice, these take the form of harassing and intimidating online communication – for example, in the case of women, by highlighting negative stereotypes or gender-based insults. It is therefore important to underline that the activities that fall into the overlapping categories of hate speech and cyberbullying can take the form not only of text or audio, but also of visual communication. Indeed, given the changes in the channels of interpersonal information transmission and the fact that communication in a visual language is much easier and faster to absorb, their role and importance in the online space is increasingly dominant. But even when used ‘only’ as a supplement, they can override the interpretative framework of the written text. In face-to-face interactions, verbal channels take a back seat to non-verbal channels. In the online space, many of these – such as tone, volume, mimicry, gesticulation, or even proxemics – are missing, and can be replaced by artificial visual elements.²⁹ An emoticon placed in a given context or sentence structure can give a completely different, even offensive, humiliating, etc., interpretative framework to an otherwise neutral verbal message.

While hate speech and cyberbullying are by no means the same set of toxic behaviors, they do show significant commonalities, particularly in the world of social media.

The risks of online hate speech are particularly significant because of several features, which are also discussed in this chapter: the anonymity of the online space, the low chances of detection, identification, ‘getting caught’ and

27 Raphael Cohen-Almagor, 2011. pp. 1–2.

28 For a discussion of the concept, see for example Anderson – Barnes, 2022.

29 For the socio-emotional needs in online communication, see Wallace, 2002. pp. 34–36.

the fact that the perpetrator does not have to face the consequences of the impact of hurtful statements on the potential victim, allowing their emotions and passions to run high without social barriers.

At the same time, the limits of fundamental rights that are considered of paramount importance in the online space, such as freedom of expression, constitute a challenge as well, in particular, if we take into account the specific, potentially distorting characteristics of text comprehension and processing – i.e. the different inferences and emotional reactions resulting from the absence or limited nature of non-verbal channels or, for example, the highly (sub)culture-dependent interpretative frameworks of complementary visual representations. While the Internet as a communicative space is supranational, the interpretation and perception of the messages sent there is very much ‘national’, influenced by cultural, cultural-anthropological, socio-psychological, historical, etc. factors. And since the main actor in judging the harassing, offensive, intimidating, etc. nature of an interaction is the specific individual or group of individuals, newer and newer aspects and filters are introduced in the process, giving more and more room to human, biological and psychological characteristics that reinforce subjectivity.

There are no universal, universally accepted, strict answers. “Now each man judges well the things he knows, and of these he is a good judge.” writes Aristotle in his *Nicomachean Ethics*.³⁰ Judgments, evaluations and boundaries vary from society to society, from age to age, influenced by historical circumstances and cultural norms. In judging the specific nature of a particular behavior, the rule of the golden mean, which Aristotle considered to be the basic tenet of a life of moderation, may be a guiding principle. Freedom of expression and opinion must therefore be allowed. But this must not be without limits: it cannot harm the honor and dignity of others.

However, an important aspect in judging hate speech is to define the concept of hate. In this case, harassment is defined as the single or repeated intimidatingly offensive behavior of a perpetrator in a position of authority in the online space, ‘which is motivated by an offender’s prejudice against a person or community and which incites or encourages hatred, discrimination or hostility towards that person or community’. As for the hate element, we have taken the interpretation of the Hungarian Constitutional Court³¹ as a basis, according to which it is “*one of the most extreme negative, [...] highly hostile emotions.*”

³⁰ Aristotle, 1987, p. 7.

³¹ Decision 30/1992 (26 May 1992) AB.

Summary

The definition of the phenomenon encompassed by abusive, harassing behavior has undergone several changes since it first became a focus of academic interest. There are several reasons for this. Changes in social and economic conditions have in themselves constantly shaped the socio-psychological attitudes of citizens and, through them, the concrete forms in which the phenomenon is realized. Among these environmental influences, the emergence and spread of technology, the Internet and information and communication tools, which have had a drastic and decisive impact – also in relation to the problem under study, should be highlighted. As research has progressed, the body of knowledge available to professionals has deepened, and conclusions and theoretical approaches have evolved as a result.

Harassment, mobbing and bullying are just some of the terms used by professionals (in some cases with slightly or considerably differing content). The diversity of these definitions reflects both the diversity of the phenomenon and of the professional focus (partly depending on the discipline), and also gives the authors the opportunity to analyze the source material available to them by highlighting a particular term.

The chosen definition of cyberbullying is defined as any attack aimed at intimidating the victim, carried out in the online space, using electronic means, with a one-off or repeated behavior, and characterized by a lack of balance of power in the relationship between the parties.

In the light of the comparative (criminal legal) focus of the book, the phenomenon contains any attack intended to intimidate the victim, carried out in online space, using an electronic device, by means of a one-off or repeated behavior, and characterized by a lack of balance of power in the relationship between the parties.

Bibliography

- Anderson, L., Barnes, M. (2022) Hate Speech. *Stanford Encyclopedia of Philosophy* [Online]. Available: <https://plato.stanford.edu/entries/hate-speech/> (Retrieved 01 December 2024).
- Antipina, S., Bakhvalova, E., Miklyaeva, A. (2020) 'Psychological Determinants of Cyber-aggression in Institutionalized Adolescents', *Young Scientists Symposium*, pp. 402–414.
- Aristotle (1987) *Nikomakhoszi etika (Nicomachean Ethics)*. Budapest: Európa Könyvkiadó
- Corcoran, L., Mc Guckin, C., Prentice, G. (2015) 'Cyberbullying or Cyber Aggression? A Review of Existing Definitions of Cyber-Based Peer-to-Peer Aggression', *Societies*, 2015/5, pp. 245–255.
- Cohen-Almagor, R. (2011) 'Fighting Hate and Bigotry on the Internet', *Policy & Internet*, 3(3) pp. 1–26.
- Cyberbullying vagy internetes zaklatás? (Cyberbullying or cyberbullying?) UNICEF [Online]. Available: <https://unicef.hu/cyberbullying> (Retrieved 03 December 2024)
- Csemáné Váradi, E. (2019) 'A digitális világtól az offline valóságig. Gondolatok a GTA apropóján', *MJSZ*, 14(2k.sz.) pp. 177–194.
- Csemáné Váradi, E. (2021) 'Közösségi media és autoagresszió – interdiszciplináris kitekintés', *MJSZ*, 16, pp. 95–112.
- 1488/2016. (IX. 2.) Korm. határozat a Gyermekek számára biztonságos internetszolgáltatás megteremtéséről, a tudatos és értékteremtő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról [1488/2016 (IX. 2.) Government Decision on the Creation of a Safe Internet Service for Children, on the Conscious and Value-Creating Use of the Internet and on the Digital Child Protection Strategy of Hungary]
- Hinduja, S. K., Patchin, J. W. (2024) *Bullying Beyond the Schoolyard – Preventing and Responding to Cyberbullying*. Thousand Oaks (CA): Corwin Press
- Kulcsár, G. (2024) *Bullying és cyberbullying. Hogyan előzzük meg és kezeljük az iskolai és az online kortársbántalmazást? (Bullying and cyberbullying. How to prevent and tackle bullying in schools and online?)*. Budapest: Novissima Kiadó
- Menesini, E., Nocentini, A., Palladino, B. E., Frisén, A., Berne, S., Ortega-Ruiz, R., Calmaestra, J., Scheithauer, H., Schultze-Krumbholz, A., Luik, P., Naruskov, K., Blaya, C., Berthaud, J., K. Smith, P. (2012) 'Cyberbullying definition among adolescents: a comparison across six European countries', *Cyberpsychology, Behavior, and Social Networking*, 15(9), pp. 455–463.
- Monori, Zs. É. (2016) 'Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái' ('Is cyberbullying

- harassment? The dilemmas of criminalising cyberbullying’), *In Medias Res*, 5(1), pp. 246-261.
- Nakano, T., Suda, T. Okaie, Y., Moore, M. J. (2016) Analysis of Cyber Aggression and Cyber-bullying in Social Networking. 2016 *IEEE Tenth International Conference on Semantic Computing (ICSC)*, February 2016 [Online]. Available: https://www.researchgate.net/publication/301710339_Analysis_of_Cyber_Aggression_and_Cyber-Bullying_in_Social_Networking
- Nocentini, A., Calmaestra, J., Schultze-Krumbholz, A., Scheithauer, H., Ortega, R., Menesini, E. (2010) ‘Cyberbullying: Labels, Behaviours and Definition in Three European Countries’, *Australian Journal of Guidance & Counselling*, 20(2), pp. 129-142.
- Olweus, D. (1999) ‘Az iskolai zaklatás’ (‘Bullying in schools’), *Educatio*, 8(4), pp. 717-739.
- Parti, K. (2016) ‘A megfélemlítés (bullying) szabályozása Magyarországon és külföldön (‘The regulation of bullying in Hungary and abroad’), *In Medias Res*, 5(1), pp. 114-146.
- Pongó, T. (2021) *A cyberbullying és a diákok véleménynyilvánítási szabadsága, különös tekintettel az USA jogrendszerére (‘Cyberbullying and students’ freedom of expression, with special reference to the US legal system’)*. Szeged: Iurisperitus Kiadó
- Preuß, T. (2019) ‘Erforderlichkeit der Kriminalisierung des Cybermobbings – Sinnvolle Schließung einer Gesetzeslücke oder bloßes Symbolstrafrecht?’, *Kriminalpolitische Zeitschrift*, 4(2), pp. 97-104.
- Schenk, L. (2020) ‘What is cyberbullying?’ in Böhmer, M., Steffgen, G. (eds.) *Bullying in schools. Measures for prevention, intervention and aftercare*. Berlin: Springer. pp. 273-301.
- Smith, P. K. (2014) *Understanding School Bullying: Its Nature & Prevention Strategies*. New York: SAGE Publications Ltd
- Wallace, P. (2006) *Az internet pszichológiája (The psychology of the internet)*. Budapest: Osiris.

III. AT INTERSECTION OF DISCIPLINES – THE JUSTIFICATION OF A HOLISTIC APPROACH

ERIKA VÁRADI-CSEMA

Effective action against the behaviors at the heart of this volume – be it cyberbullying or hate speech – is unthinkable without exploring the causes behind the phenomenon, analyzing the characteristics of the perpetrators, and reviewing the risk factors of becoming a victim. This is of paramount importance not only in terms of prevention and the use of (criminal) legal and extra-legal instruments but also in terms of resolving the consequences of victimization.

1. Cyberbullying

The literature on cyberbullying, in addition to a general analysis of the phenomenon, focuses on minors as the group most at risk of becoming victims (and perpetrators)¹. The various national crime prevention strategies², international documents³, EU⁴ and national regulations⁵ also make considerable efforts to protect the interests of the new generations⁶ in the fight against cyberbullying. Hungary, for example, has an independent Child Protection Strategy⁷ which, in

1 From the first steps (e.g. Visionaries Project, 2006; Sorrentino et al., 2019; Bruckmayer, 2020) until nowadays (e.g. Kulcsár, 2024).

2 Niestadt, 2022.

3 Murphy, 2024b.

4 See e.g. Murphy, 2024a.

5 Henares-Montiel, 2024.

6 See e.g. Negreiro, 2023.

7 The Digital Child Protection Strategy of Hungary.

addition to addressing the main issues of the phenomenon, also defines specific forms of prevention (treatment) and options for response.

In order to deal with and prevent cyberbullying as effectively as possible, the document draws on the findings of international criminological research⁸, which have in common the use of technology for the purpose of harassment.

The phenomenon is extremely diverse and, for various reasons, constantly changing in nature, giving rise to different typologies. According to one main theoretical approach, there are several forms, some of which are indicated in the Strategy⁹, e.g.

- (a) flaming: flaming is an on-line ‘fight’ in which angry, threatening or vulgar messages are sent in masse to the victim;
- (b) repeated harassment: means the repeated or continuous sending of rude, abusive, crude and insulting messages, usually anonymously;
- (c) dissing is a form of defamation and means the sending of on-line messages which are likely to damage the reputation of the victim (for example posting drawings, reports or comments on platforms such a school websites that ridicule or question an individual’s sexual abilities);
- (d) impersonation: impersonation is aimed at damaging the victim’s friendships, romantic relationships and social connections by sending messages, text messages, etc. on their behalf (e.g. by obtaining their password), thereby harming their reputation;
- (e) outing and trickery sharing: a distinct form of cyberbullying, where the perpetrator fraudulently obtains and shares the victim’s secret or embarrassing information or concealed characteristics (e.g. secretly taking nude photos of a victim who changes clothes in a separate room due to severe obesity and then sending these pictures to peers or posting them on the internet);
- (f) intentional exclusion: means excluding someone from a particular on-line group (e.g. chat room);
- (g) *cyberstalking*: stalking the victim in cyberspace on a continuous, repeated basis by sending threatening or extremely intimate messages or by conducting other on-line activities that violate or endanger the victim’s safety (e.g. sending messages to the victim’s friends or strangers with pictures of the victim’s erotic or sexual activities, with the victim’s e-mail address and e.g. skype name, without the victim’s consent).

⁸ See more about the research-activity in Kulcsár, 2024.

⁹ For more details see Csemáné Váradi, 2016. pp. 627–661.

Other classifications of cyberbullying types are partly different.¹⁰ According to these, cyberbullying can basically be categorized into a few main types, such as

- (a) social exclusion,
- (b) unauthorized tagging,
- (c) humiliation (burning/'flaming'),
- (d) sext re-posting (sharing intimate sexual messages), and
- (e) impersonation and identity theft.

Although exclusion is by far the least abusive of these behaviors, it also has the potential to cause distress and frustration. The essence of unauthorized tagging is that the person is associated with a typically degrading image shared online without their consent and the mechanism by which the sharing platforms work causes these degrading images to be attached to images uploaded and tagged by the victim. Flaming, or burning or humiliation is a dominant and common tool of character assassination. The re-sharing of sexually explicit texts exchanged during intimate interactions poses a significant risk of victimization, particularly for younger age groups. When such content is disseminated in visual form, the psychological harm inflicted is even greater.

The range of abusive behaviors is constantly evolving, partly as a result of technological developments and user habits, and partly as a result of the growing knowledge base of researchers. Accordingly, in addition to the laming of people by sending abusive messages in the hope of provoking a reaction, a new approach is being developed, for example in Cuncin's categorization:¹¹

- (a) outing: disclosing (typically in a larger circle) private information that is embarrassing or uncomfortable for the person concerned,
- (b) trolling: typically the sharing of some degrading, defamatory statement or opinion about a person or group, with the aim of annoying a wider audience of users (not just the people concerned!), usually with the aim of provoking an emotionally charged, embarrassing online reaction,
- (c) name calling: calling another person an insulting, degrading name, referring to them by that name in other online interactions (particularly significant among young people (42%)¹²

¹⁰ Hochstetler, 2016.

¹¹ Cuncin, 2022.

¹² Anderson, 2018.

- (d) spreading false rumors: spreading untrue stories, ‘truths’ or allegations about a person (second most common among young people, with 32% prevalence)¹³
- (e) sending explicit images or messages: sharing intimate (indecent) images or messages about the victim without the victim’s consent
- (f) cyber stalking/harassing/physical threats: repeatedly stalking, harassing or threatening to physically assault a person (reported by 16% of young people¹⁴ having experienced the latter).

The use of mobile phones and their use as cameras for unauthorized purposes is also becoming increasingly common. It is not only in PE lessons or training sessions that pictures of people who are naked or underdressed can be taken and sent to each other or uploaded to the internet, but also on school trips or at parties. Specific phenomenon among cyberaggression cases are ‘Happy Slapping’ videos and ‘Snuff Videos’.

First detected in the UK, these “forms of entertainment” were initially perpetrated in schools against students but now virtually anyone can be targeted. ‘*Happy Slapping*’ is the practice of forcing a usually defenseless victim to engage in humiliating activities, but nowadays it is more likely to involve the hitting, punching or kicking of a victim, which is photographed or filmed on a mobile phone and then sent to friends in the form of a photograph or video clip, or posted online. In London, for example, a 37-year-old man working as a barman was attacked by 4 boys while sitting in a park. The victim eventually died from the kicking and punching¹⁵. However, in this case, the use of violence was not the main purpose of the act but rather the making and forwarding of the footage, which was used to raise the perpetrators’ profile. This is illustrated by the behavior of a 14-year-old perpetrator who, after kicking the victim in the head, pleaded with his victim on the ground: “We are making a documentary, so please look into the camera.”

In the first period after the problem-behavior appeared, the target of ‘happy slapping’ acts could typically be anyone who was a little different from the ‘average’ (as one perpetrator put it, if somebody looked a little bit ‘stupid’). The victims were typically students. Later, however, teachers¹⁶ also appeared among the victims, although still in smaller numbers.

¹³ Anderson, 2018.

¹⁴ Anderson, 2018.

¹⁵ Grimm, 2006.

¹⁶ For many similar cases, see for example: Happy slapper boy behind bars. *Shropshire Star*, 11 August 2008 [Online].

A similar motive is behind the so-called ‘*snuff videos*’. The name comes from the English word ‘to snuff out’, which literally means to snuff out, to cough up one’s soul. The physical or psychological humiliation, rape or beating of the victim can then be recorded as a form of body snuffing (shocking footage of the victims/victims at the scene of fatal road accidents, crimes, suicides can be found on the internet).

‘Snuff videos’ have also been around for some time, so there are many examples. Some of them are related to the immediate environment and the way of life of young people, and can often be linked to various types of sexual assault.

The victims are mostly young women in a drunken state and the phenomenon is linked to ‘rape culture’. Rape culture has been identified particularly among young people, and is characterized by a higher tolerance of abusive sexual behavior; among typically young male perpetrators the (unlawful) act has positive perception; for typically female victims it is associated with the risk of casual partnerships, parties in dormitories and schools, and alcohol consumption. Some experts identified five important elements behind the attitudes of young people¹⁷. These are traditional gender roles, sexism, hostile sexual beliefs, hostility towards women and the acceptance of violence as a means to an end. This phenomenon has taken on a new level with the advent of the internet¹⁸ and the increasing role of social media.

It is worth noting that cyberbullying and rape culture are a specific offshoot of new hyper-realistic technologies¹⁹ such as VR goggles. Thanks to the high degree of realism, harassing attacks in virtual space can produce the same negative psychological effects²⁰ as real-life victimization even without the actual physical touching of the body. Game manufacturers are trying to combat these situations. For example, in the multiplayer version of the fantasy game QuiVR²¹, a special ‘protection’ bubble has been created which, when used, prevents such attacks.

Although not all students agree with the actions, they receive and transmit such videos and images because they believe that by doing so they can become interesting, known, a ‘somebody’ to others thus they can avoid being left out of peer-activities. To understand the importance of the media, the Internet and participation in communication, it is necessary to know the socio-psychological, cultural-anthropological, etc. characteristics of the younger generations. Although there are significant differences between different groups and strata

17 Johnson et al., 2021, p. 70.

18 Holladay et al., 2019, p. 80.

19 Gillespie, 2020.

20 Carrie, 2016.

21 For the game see: <https://blog.vrplayin.ca/quivr-multiplayer-content-series>

of young people, in terms of their financial resources, learning and employment opportunities, there are numerous characteristics that distinguish those born after 1995 from earlier age groups.

2. Causes and effects

Although the causes behind cyberbullying are wide and varied, but there are some common characteristics of the internet, of social media and of the ICT, that are generally – and particularly among young people – could be a relevant risk factors of phenomenon, such as

- (a) easy accessibility,
- (b) increasing psychological dependence on new technologies (e.g. USA, Australia, New Zealand, Central Europe),
- (c) ICT and social media are part of the socialization process, they are important spaces for social interactions,
- (d) the absence of consequences (the ‘perpetrator’ is not always identifiable, rarely followed by criminal sanctions),
- (e) tolerance of violence; general social communication is also more violent – i.e. violence is an accepted behavior, it can also be a parenting pattern for young people
- (f) violence is an accepted social or peer pressure tool for young people,
- (g) lack of control by the community, the immediate environment, the parents,
- (h) the possibility of anonymity,
- (i) the lack of a tangible background,
- (j) the media’s cult of violence, the value-positioning of violence (heroes, saviors, ‘punishers’ in the name of justice),
- (k) patterns of bullying behavior (‘bully’ in a PC/Xbox/Psp game ‘Bully’ where you have to play the school bully in a school; the school itself is called ‘Bullworth Academy’).

The particular danger of online bullying, as Gabriella Kulcsár²² claims in her study, is not only the anonymity of the perpetrator, but also the large potential audience for the harassment. It is particularly important to note that some of the online harassers have themselves been victims of direct harassment in the past and have subsequently chosen this form of communication to vent their frustration with

²² Kulcsár, 2022, pp. 31–41.

their victimhood. The general perception of communication in the online space is that aggressive user behavior is more prevalent on this platform, especially in the context of anonymity, which can lead to potential cyberbullying. Research on some social networks²³ have clearly shown that anonymous users exhibit more aggressive behaviors than those who assume their identity.

The aggressive content of the response to rude comments also depends on anonymity. Respondents to an aggressive question asked anonymously also show a higher level of aggression than asking a question from a non-anonymous user with a similar attitude²⁴. However, an important finding is that aggressive user behavior alone is not necessarily linked to cyberbullying. The latter phenomenon has a number of elements that are not inherent in the use of obscene or offensive language or communication style.

In the case of those who participate in harassment as ‘relays’, i.e. silent contributors, the reasons are very diverse²⁵. However, most researchers clearly attribute the unstoppable spread of this form of violence to a crisis of values²⁶ and a distorted image of success in the media. Students receive and transmit such videos and images because: ‘I can show off in front of the others’. It is also important that they are not left out of the communication (‘so I can have my say’). As long as these behaviors are able to elicit respect and recognition from acquaintances and peers, the rate of this phenomenon will not decrease.

The potentially devastating impact of the Internet and its activities, the vulnerability caused by an inadequately thought-out or careless social media presence, is a factor that is difficult for a large proportion of young people to grasp and understand. Yet cyberbullying, anonymous, rude comments, mocking others, can be a serious psychological trauma for the person concerned – especially if we consider that the majority of users living in the virtual world, are psychologically attached to it, and feed off of positive feedback and praising they receive. There are now several cases of young people who have seen suicide²⁷ as the only way to protect themselves from the harassment they have experienced and been unable to deal with, or from constant abusive attacks. The case of Amanda Todd is particularly shocking. A month before her fateful decision, the 15-year-old Canadian girl ‘told’ her story in a YouTube message, explaining the cause of her depression, her hopelessness, her antidepressant overdose, her self-harming actions and asking for help (“I have no one ... I need someone”). Help was absent,

²³ See for example Brown, 2018, pp. 297–326.

²⁴ See for example Brown, 2018, pp. 297–326.

²⁵ Csemáné Váradi, 2009, pp. 84–95.

²⁶ Several studies have addressed the issue of moral crisis, such as Cordero, 2013; Duff, 2012.

²⁷ Csemáné Váradi, 2014, pp. 90–91.

as in the case of 12-year-old Lara Burns, where similar harassing messages led to a fatal outcome. Although bullying/cyberbullying is a very serious risk factor for suicidal ideation and attempts, it takes a combination of many factors to lead to such a tragedy. It is important to look at the other factors as well when investigating these cases to get the full picture²⁸ to prevent further incidents. (Although for other reasons, it is also a serious risk if young people accept cyberbullying and tolerate rude, derogatory language, saying that this is the norm on the social networking site, that it is natural, that everyone behaves like that.)

The specific manifestation and impact of this phenomenon depends on age. Equally important as an age-specific factor is the specificity of the online world – i.e. the quality of the messages conveyed by the entertainment options preferred by young people. Imagery – whether gifs, memes, and video content uploaded to YouTube channels or images available on Instagram – is a key part of young people’s communication. In this respect, there are several problems regarding the content of messages. The amount of violence, particularly in audiovisual format, the one-sided portrayal of crime and other deviant behaviors, the value and impact of stereotypical representation are often undesirable. The existence and content of school bullying, physical bullying, ‘happy slapping’, ‘snuff videos’, makes young people tolerant of abusive behavior and reduces empathy. The creation of online content that makes fun of everything, including the other person’s physical and mental state of distress, and is built on fear, vulnerability and helplessness of the other party, is based on a ‘basic principle’ of the virtual world and social media: only those who are ‘on’ the net exist. Those who are successful and have many followers are worth something, and collect likes. The information society’s image of society, which is also reflected in young people’s visual communication and is divided into winners and losers, can lead, among other things, to serious self-esteem and relationship problems, and to a system of values and norms that is undesirable²⁹. Moreover, the need to be constantly present in the online social space, the loss of intimacy, emotional incontinence, the loss of the ‘right to be forgotten’ can cause tension, anxiety and can also lead young people more easily into forced roles and victimization. The dissolving of moral barriers, the impersonal nature of e-communication³⁰ and its specific characteristics make it easier to humiliate and offend the other party without the ‘offender’ being aware of the seriousness of the offence and his or her own responsibility.

28 On the interaction between school bullying and adolescent suicide, see Kulcsár, 2018, pp. 426–433.

29 For more details, see King – Horwitz – Berona – Jiang, 2013, pp. 43–50.

30 Subrahmanyam – Greenfield, 2008, pp. 119–203.

Cyberbullying as a public health risk factor³¹ can also be named as a health risk. Numerous studies have shown that victimization can lead to a persistent sense of fear, generalized anxiety, social isolation and poorer performance at work and at school. Indirect effects may even include difficulties in establishing interpersonal interactions. Given the persistence of information in the online space and the lack of the right to be forgotten, victims are unable to cope with the psychological impact of victimization, partly due to fear and due to the repetitive nature of the harassment, and this can lead to severe post-traumatic stress disorder³² long term, resulting in depressive symptoms.

The psychological effects of cyberbullying, regardless of age, are wide-ranging and might have a significant impact on the mental health of the victims, particularly adolescents who are exposed to it. Fact, that among adolescents poor psychological adjustment reactions, low trauma coping skills³³, and the lack of the coping strategies and psychological support are associated with previous victimization, low self-esteem and suicidal ideation/thought. This correlation is more stronger among youngsters, then among adults.

However, victimization has a negative impact not only on psychological but also on physical health.

The need to belong to an online community is age-independent; however, the need to belong – and thus the risk of victimization – is particularly strong in young people.

There is also a gender difference³⁴ between both the perception of harassment and the frequency and inappropriate response to victimization. Girls report higher cybervictimization experiences more often, while inappropriate psychological reactions (like e.g. drug, alcohol abuse, suicide thoughts) to cybervictimization occur more often in boys.

For young people, the negative impact may be more significant and severe for additional reasons. An age-specific feature of young people's communication is that most of them have a clear problem in managing and expressing their emotions, recognizing and identifying the causes.

Communication barriers, the inability to talk about feelings and emotions and thus to reduce internal psychological pressure, may even lead to self-harming activities (e.g. walling). As a result of self-injurious behavior, pain becomes localized, identifiable – and thus 'manageable'. But this behavior may be seen by the young person as a form of self-punishment (e.g. self-hatred), as a means

31 Chengyan – Huang – Evans – Zhang, 2021, pp. 1–12.

32 Datta – Gupta, 2021, pp. 88–91.

33 For the importance of this, see Kulcsár, 2021, pp. 136–145.

34 Extremera – Quintana – Orts – Mérida-Lopez – Ray, 2018, pp. 367–376.

of coping with stress or as a way out of a situation that is beyond their control (e.g. head-butting to the point of unconsciousness in a dysfunctional family)³⁵.

Various forms of cyberbullying among young people multiply the already severe effects of bullying at school. The most common manifestations accompanying school violence and bullying have been identified as early as the 2000s³⁶:

- Breaking social and community rules (feeling of not belonging, being rejected, not recognizing the situation, not knowing the rules, not being able to respect boundaries);
- severing family ties, ‘leaving’ the community, being trapped in gangs, groups, elders;
- defending a wounded sense of self by attacking (neglect of the school as an organization and its staff, defiance, attacking other children – who are more integrated and weaker –, bullying, leaving school);
- loss of a positive self-image (associated with the emergence of potentially destructive, self-mutilating, self-destructive behavior, self-hatred).

In the light of these factors, it is understandable that the behavior and signals of children and pupils in trouble at school should be recognized and interpreted by those working there, and should be seen primarily in terms of what it actually means, not how it is expressed.

In fact, the virtual space, and social media in particular, has a number of specificities, depending on which different links to auto-aggressive behaviors can be identified.³⁷ Among other things, self-harming behaviors that are not suicidal are also underpinned by self-critical rumination³⁸, the chances of which are increased by earlier cyber-victimization. The young person’s constant ruminations on his/her own external/internal faults and shortcomings have a negative impact on both his/her physical and psychological well-being, but their significance is even greater; their prolonged presence is closely associated with the onset of anxiety and depressive symptoms³⁹, which are risk factors for suicidal urges. It is important to highlight two elements in this respect. First, that already in 2017 surveys⁴⁰ have confirmed that the increase in time spent on social media, especially Facebook, increases the presence of anxiety disorder among 18-23 year olds present on the platform. On the other hand, Instagram

35 Csemáné Váradi, 2021, pp. 102–103.

36 Research on violence among children [Online]. Available: <https://osztalyfonok.hu/344/> (Retrieved 30 June 2022).

37 Based on Csemáné Váradi, 2021, pp. 95–112.

38 Reinhardt et al., 2021, pp. 531–532.

39 Kocsel, 2019, p. 28.

40 For a description of the research, see Vannucci – Flannery – Ohannessian, 2017, pp. 163–166.

encourages users to constantly compare themselves with others, which can result not only in a negative self-image but also in a decrease of self-esteem.

On the other hand, suicidal impulses often lead young people to look to ICT platforms for solutions. A specific form of harassing and abusive behavior on the Internet, which is also relevant from the point of view of *criminal law*⁴¹, can be, when a person who seeks help or has already committed self-harm on social media, or attempted the most serious form of self-harm, i.e. suicide, is psychologically abused, emotionally humiliated and encouraged to carry out the behavior (e.g. suicide), which may even lead to the loss of his or her life.

This can also be a form of online bullying and harassment, which is relevant for the assessment of criminal liability, when a person seeking help or already engaging in self-harming behavior or the most serious form of self-harming behavior, i.e. suicide, is emotionally abused, emotionally humiliated and encouraged to carry out the behavior, which may even result in the loss of his or her life.

In general, and regardless of age, cyberbullying has a negative impact on depression, mediated by an increased fear of being alone⁴². The more intense the fear of loneliness, the more vulnerable and defenseless the person may become in the online space – increasing the impact of abusive online behavior.

3. Focus on hate speech

Hate speech, as a category in its own right, is in fact a type of online communication with a hostile attitude, characterized by the insulting of the honor of a person, persons or social groups, and the degrading of the community. Given this strong negative emotional attitude, the specific impacts of hate speech⁴³ may vary depending on the strength of a person's affiliation with the target group (how much of their identity is about where they belong, e.g. self-identity as a woman). The extent of the impacts also depends on the degree of involvement of the person. For example, previous victimization or a sense of threat experienced in the context of social identity increases sensitivity to hate speech. Typically, victimization has psychological consequences similar to other traumatic experiences, i.e. frustration, psychological stress, depressive symptoms, but often also anger as a consequence of negative emotions such as fear. In general, i.e.

41 For a more detailed description of cyber suicides and user reactions, see Csemáné Váradi, 2021, pp. 95–112.

42 Varela – Hernández – Miranda – Barlett – Rodríguez-Rivas, p. 5886.

43 Schmid et al., 2022, pp. 4–5.

regardless of culture or gender, it is true that individuals are much less likely to perceive the sharing of their own opinions as hate speech than the reverse⁴⁴. The specific 'form' of hate speech is also important when it comes to counter-ing it; degrading, offensive, visual representations have a greater impact among social media users than among other individuals⁴⁵. Individuals with lower resilience are more vulnerable to emotional outbursts and, in this context, have been shown to be more neurotic than their more resilience-affected counterparts⁴⁶ – online hate speech is more prevalent – by about 25%(!) – in this group of students than in other groups of similar age. It is interesting to note, however, that in some communities that are more challenged or more sensitive to social and community issues and have a higher stress factor associated with these issues, such as college students⁴⁷, have also shown that some social groups, such as minorities or immigrants, have higher rates of exposure to hate speech⁴⁸. This also predicts a higher likelihood of developing symptoms of post-traumatic stress disorder and depression, which are mediated by 'acculturation stress'⁴⁹. A common feature is that the extent of this is particularly high in the case of discrimination in the form of hate speech. Acculturation⁵⁰ itself is a dual process of cultural and psychological change that occurs as a result of contact between two or more cultural groups and their individual members that involves various forms of necessary mutual adaptation. These in turn lead to longer-term psychological and socio-cultural adaptation – or the need for it. According to acculturation psychological theory, the psychological health of individuals changes as they adapt to a new cultural environment.⁵¹

It is important to note, however, that perceptions of and sensitivity to hate speech have declined significantly in recent times, particularly in the context of the emergence of social media⁵², by more frequent use of social media leading to lower perceptions of hate speech. Another important finding is that those who are less sensitive to the perception of hate speech are less likely to experience the associated negative psychological effects. Research following the emergence of social media has shown that this platform is a space for aggressive

44 Schmid et al., 2022, p. 4.

45 Schmid et al., 2022, pp. 11–12.

46 See for example Saha et al., 2019, pp. 255–264.

47 Saha et al., 2019, p. 255.

48 For more details, see Wypych – Bilewicz, 2022.

49 Acculturation stress is the result of the conflict situation that an individual experiences when adapting to the new culture of the host society. See Berry, 1997, pp. 5–34.

50 Berry, 2005, pp. 698–699.

51 Ren – Jiang, 2021, p. 4751.

52 Schmid et al., 2022.

communication, conflict-generating hostility and interpersonal interactions imbued with humiliating hostility.

Not only the frequency of social media use, but also the age of the specific user and the communication/cultural characteristics of the community are decisive. For example, 64% of US youth aged 13-17 have encountered hate speech, compared to only 18% of New Zealand adults aged 18 and over. Youths typically have high rates of using derogatory attitudes towards a collective⁵³. However, regardless of the country, it is true that the proportion of hate speech is increasing steadily, for example in Germany it reached 78% by 2021⁵⁴. Of course, another trend can be observed in contrast to the increase in tolerance levels already mentioned. Thanks to conscious campaigns and the increasing human-rights communication aspects of recent times, the range of concepts falling under the category of hate speech is widening.

4. Perpetrators and victims

In addition to the effects of abuse, harassment and bullying in the online space, it is important to identify its possible causes in order to ensure effective prevention.

There are several very different influencing factors that may be involved in becoming an offender. In this context, it is particularly important to identify the specific causes of bullying and its contribute factors.

The *specific causes* may include a number of actors with very different characteristics⁵⁵. One of these is boredom, which can be banished by using a mobile phone. A similar special opportunity provided by ICT platforms is the possibility of trying out a new identity⁵⁶. The user can assume the ‘avatar’ of anyone, and thus play any role (even an ‘evil’ one) without any direct consequences.

It is interesting to note that negative experiences, even earlier victim situations⁵⁷ can lead to becoming a bully. Previously experienced offline victimization can generate online bullying activity, as can feelings of loneliness and abandonment. Being an outsider, living in isolation is very hard – especially in adolescence -, so they choose this way to draw attention to themselves.

53 Schmid et al., 2022, p. 2.

54 Schmid et al., 2022, p. 2.

55 Cuncin, 2022.

56 For evidence, see Varjas – Talley – Meyers – Parris – Cutts, 2010, pp. 269–273.

57 Slonje – Smith – Frisé, 2013, pp. 26–32.

However, they can also project their feelings of hostility and anger towards their immediate environment onto society⁵⁸, thus improving their well-being. While in these cases anonymity and a large or randomly selected target group/individual are more typical, perpetration due to a break-up or relationship breakdown is typically a targeted attack. Here, the actors are ‘parties’ (usually former friends or partners) who have experienced conflicts in their friendship that they could not or did not want to deal with, or have had a breakdown in their relationship, for example because of jealousy. In such cases, the specific motivating force is often revenge⁵⁹.

A special group of abusers are those with psychologically or psychiatrically relevant personality traits, disorders or illnesses that induce abusive behavior online⁶⁰. Examples include those with aggression, hyperactivity or impulsive-control disorders. Substance abuse, such as alcohol or drug addiction, can also generate such mental health problems (i.e. it is not a case of a person harassing or humiliating a victim with online messages while under the influence of alcohol or drugs). International research⁶¹ has shown that these pathologies can be a risk factor for cyberbullying behavior, even for users of different ethnicities (Asian, black and white). However, for each of these groups, the correlation was found to be lower for women, even with any of the symptom complexes studied. Although these personality disorders can be described by very different traits, they share common characteristics such as a typically low level of empathy and the use of bullying as a technique to boost self-confidence or to gain a position of power. (Otherwise, the presence of users with narcissistic personality traits is over-represented on social media⁶², but this does not necessarily imply the existence of an active bullying status.)

The ‘dark tetrad’ may even play a mediating role⁶³. The term’s predecessor, the ‘dark triad’⁶⁴, was coined by two Canadian psychologists. In 2002, Delroy Paulhus and Kevin Williams concluded that three negative personality traits with partially distinct characteristics could be identified that could play a significant role in the identification of certain aversive, deviant, norm-breaking or law-breaking behaviors. While Machiavellianism is characterized by a tendency to manipulative behavior, narcissism by excessive self-confidence, and

58 Hermens – McLoughlin, 2018, pp. 1–7.

59 König – Gollwitzer – Steffgen, 2010, pp. 210–224.

60 Skilbred-Fjeld – Reme – Mossige, 2020, pp. 1–16.

61 For a more detailed description Brown – Hazraty – Palasinski, 2019, pp. 552–557.

62 Craker et al., 2016.

63 Kircaburun – Jonason – Griffiths – Aslanargun – Emirtekin – Tosuntaş – Billieux, 2021, NP1877– p. 1893.

64 Furnham et al., 2013.

psychopathy by callousness and impulsivity. This is because all three personality traits are characterized by self-assertiveness, emotional coldness, duplicity and aggressiveness. In 2019, the term was extended to include sadism, creating the term ‘dark tetrad’. According to research, “Dark personality traits (Machiavellianism, Narcissism, Psychopathy, and Sadism) have been associated with aversive, unethical, and criminal behavior”⁶⁵.

The ‘dark tetrad’ can also be an intermediary between the role of victim and perpetrator, although the strength of this relationship varies depending on biological sex.

Even with the same childhood victimization, it is true that the reported personality disorders led to higher rates of cyberbullying in males than in females. However, the extent to which these traits are able to predict the relationship between childhood emotional abuse and cyberbullying also depends on the type of specific personality problems along gender lines. Thus, while Machiavellianism, for example, mediates for both sexes, sadism fulfils this role fully for males and psychopathy for females. Beyond the indicated individual-specific causes, there are also the ICT platform features that increase the possibility for online bullying behavior. In the absence of these specific reasons, there are a number of reasons which are clearly present even in those who would not otherwise become perpetrators in an offline situation. There is no need to be close to the target person or group or to have any special strengths. There is no need for a prior position of power, superiority or imbalance; there is no need to be physically stronger or socially superior (e.g. more popular or wealthier), thus ensuring the support or at least the passivity of other observers. All that is needed is an internet connection and an ICT tool.

The absence of numerous barriers relevant to the activation of social inhibition is similarly supportive of perpetration. Although anonymity is important in this context, the possibility of social disapproval is not an issue. But perhaps even more importantly, the act does not involve direct confrontation, face-to-face encounters with the victim and thus confrontation with the negative effects triggered. There are no doubts of sympathy, since the victim, with all his suffering and feelings, is very distant from the perpetrator. The immediate personal interaction that can be experienced offline is also missing. In anonymous offending, the victim is usually unable to react directly to the abusive behavior, even if he or she would otherwise be psychologically capable of doing so.

65 Rassin et al., 2024, p. 311.

Summary

Cyberbullying and online hate speech are two phenomena that differ in many of their characteristics. At the same time, the era and the social circumstances that 'breeds' these norm/offending behaviors are the same. The environment created by the information society of the 21st century, the distortion of values, the change in lifestyles, are myriad factors that have had a uniform impact on members of society, its mental status and behavior. But it is not only the identity of macro- and micro-structural factors that may be the link. The two forms of behavior under study may also show a direct connection. Thus, for example, Gabriella Kulcsár⁶⁶ – also in the light of international research trends – specifically names stigma-based (cyber)bullying. In this case, the abusive, harassing behavior is based on prejudices and negative stereotypes against the other person or certain groups of persons. (Therefore, the terms *identity-based*, *prejudice-based* and *bias-based* (cyber)bullying are also accepted.) Stigmatization can be linked to a physical characteristic, personality trait, lifestyle (e.g. sexual orientation), etc. If the (cyber)bullying behavior is motivated by hatred or prejudice towards a particular group, if the perpetrator's aim is to humiliate or intimidate the victim's (perceived or real) community, *the specific behavior is at the intersection of the two phenomena*.

The two behaviors also share the common characteristic that, whatever the specific form of the abusive or harassing behavior, its psychological effects could last for a long time⁶⁷ and, without appropriate help, could be affect the victim for the rest of his or her life. Due to the specific characteristics of ICT platforms – lack of the right to be forgotten, anonymity, unrestricted flow of information, etc. – these negative consequences are multiplied many times over, regardless of the age of the individuals concerned. Over time, bullying behavior leads to problematic behavior detected by the external environment, while victimization significantly increases the risk of the development and long-term presence of health-relevant internalizing patterns such as depression or anxiety⁶⁸. Although conceptual-theoretical approaches to the phenomenon may differ⁶⁹, the legislative environment, the active intervention and responsibility of public authorities and the general perception of society play a key role.

⁶⁶ Kulcsár, 2024, pp. 63-65.

⁶⁷ For a more detailed description Marciano – Schulz – Camerini, 2020, pp. 163–181.

⁶⁸ Marciano et al., 2020, p. 1.

⁶⁹ Erdélyi, 2021, pp. 20–21.

Bibliography

- Anderson, M. (2018) 'A Majority of Teens Have Experienced Some Form of Cyberbullying', *Pew Research Center*, [Online]. Available: <https://www.pewresearch.org/internet/2018/09/27/a-majority-of-teens-have-experienced-some-form-of-cyberbullying/> (Retrieved: 06 December 2024)
- Berry, J. W. (2005) 'Acculturation: Living successfully in two cultures', *International Journal of Intercultural Relations*, 29(6), pp. 698–699.
- Berry, J. W. (1997) 'Immigration, acculturation, and adaptation', *Applied Psychology*, 1997/46, pp. 5–34.
- Brown, A. (2018) 'What is so special about online (as compared to offline) hate speech?', *Ethnicities*, 18(3), pp. 297–326.
- Brown, W. M., Hazraty, S., Palasinski, M. (2019) 'Examining the Dark Tetrad and Its Links to Cyberbullying', *Cyberpsychology, Behavior, and Social Networking*, 22(8), pp. 552–557.
- Bruckmayer M., Galimberti S. (2020) *Anti-bullying Practices from the Repository of the European Platform for Investing in Children (EPIC)*. Brussels: EPIC (EU)
- Carrie, J. (2016) *Sexual harassment in virtual reality feels all too real – 'it's creepy beyond creepy'*. [Online]. Available: <https://www.theguardian.com/technology/2016/oct/26/virtual-reality-sexual-harassment-online-groping-quivr> (Retrieved: 03 December 2024)
- Cuncin, A. (2022) *The Psychology of Cyberbullying* [Online]. Available: <https://www.verywellmind.com/the-psychology-of-cyberbullying-5086615#citation-1> (Retrieved: 03 December 2024)
- Cordero, D.A. (2013) 'Moral Decline in Teens: The Application of Contextual Theology', *Asia-Pacific Social Science Review*, 13(2), pp. 24–40
- Craker, N., March, E. (2016) 'The dark side of Facebook®: The Dark Tetrad, negative social potency, and trolling behaviours', *Personality and Individual Differences*, 102, pp. 79–84.
- Csemáné Váradi, E. (2014) '„Színlelni boldog éveket...” Gondolatok a fiatalok bűnözésének társadalmi reprodukciójához' in Borbíró, A., Inzelt, É., Kerezi, K. Lévy, M., Podoletz, L. (szerk.) *A büntető hatalom korlátainak megtartása: a büntetés mint végső eszköz. Tanulmányok Gönczöl Katalin tiszteletére*. Budapest: ELTE Eötvös Kiadó. pp. 83–94.
- Csemáné Váradi, E. (2016) 'Gyermek és fiatalkori kriminalitás' in Borbíró, A., Gönczöl, K., Kerezi, K., Lévy, M. (szerk.) *Kriminológia*. Budapest: Wolters Kluwer. pp. 627–661.
- Csemáné Váradi, E. (2009) 'Konfliktusok örvényében – a drunkorexiától a kollektív erőszakig' in Németh, Zs. (szerk.) *Írások Tauber István emlékére*. Budapest: ELTE ÁJTK, MKT, RTF. pp. 84–95.

- Csemáné Váradi, E. (2021) 'Közösségi média és auto-agresszió – interdiszciplináris kitekintés', *Miskolci Jogi Szemle*, 16(5) (3. különszám), pp. 95–112.
- Datta, V., Gupta, J. (2021) 'Cyber bullying: Causes, psychological impact and remedies', *UGC Care Group Ejournal*, 11(5), pp. 88–91.
- Duff, S. A. (2012) *A Normative Theory of the Information Society*. New York / London: Routledge ('The Normative Crisis of the Information Society' pp. 7–15)
- Erdélyi, Á. (2021) 'Az online térben bekövetkező zaklatások lehetséges okai, dinamikai jellegzetességei és megoldási lehetőségei', *Nemzetbiztonsági Szemle*, 9(3), pp. 18–32.
- Extremera, N., Quintana-Orts, C., Mérida-Lopez, S., Ray, L. (2018) 'Cyberbullying victimization, self-esteem and suicidal ideation in adolescence: does emotional intelligence play a buffering role', *Frontiers in Psychology*, 2018/9, pp. 367–376.
- Furnham, A., Richards, S.C., Paulhaus D.L. (2013) 'The Dark Triad of Personality: A 10 Year.', *Social and Personality Psychology Compass*, 7/(3) pp. 199–216,
- Gillespie, E. (2020) Virtual rape and sexual abuse: The dangers of immersive technology. *SBS News*, 11 December 2020. [Online]. Available: <https://www.sbs.com.au/news/the-feed/article/virtual-rape-and-sexual-abuse-the-dangers-of-immersive-technology/4v2n12p3f> (Retrieved: 03 December 2024)
- Grimm, P. (2006) *Mobiltelefonok csak 18 éves kortól? Pornográfia és erőszak a mobilokon*. Stuttgart: Hochschule für Medien
- Happy slapper boy behind bars. *Shropshire Star*, 11 August 2008 [Online]. Available: <https://www.shropshirestar.com/news/2008/08/11/happy-slapper-boy-behind-bars/> (Retrieved: 03 December 2024)
- 'Happy slapping' gang members admit killing Ekram Haque. *BBC News*, 16 June 2010 [Online]. Available: <https://www.bbc.com/news/10331547> (Retrieved: 03 December 2024)
- 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, p. 7364. (pp. 13)
- Hermens, D. F., McLoughlin, L. T. (2018) 'Cyberbullying and Social Connectedness', *Frontiers for Young Mind*, 6(54), pp. 1–7.
- Hochstetler, L. (2016) *Five types of internet abuse used to cyberbully*. Association of Internet Research Specialists, 13 May 2016. [Online]. Available: <https://aofirs.org/articles/five-types-of-internet-abuse-used-to-cyberbully> (Retrieved: 06. December 2024)

- Holladay, K. R., Hagedorn, W. (2019). 'The Use of Technology in Sexual Exploration Among a Rape Culture Youth', *Journal of Counseling Sexology & Sexual Wellness: Research, Practice, and Education*, 1(2) pp. 80–89.
- Jeeves, P. (2015) *Happy-slap video of boy's beating posted on Facebook but attacker gets away with it* [Online]. Available: <https://www.express.co.uk/news/uk/619050/Mother-s-fury-after-happy-slap-video-of-son-s-beating-posted-on-Facebook-but-attacker-gets> (Retrieved: 01 December 2024)
- Johnson, N.L., Johnson, D.M. (2021) 'An Empirical Exploration Into the Measurement of Rape Culture', *Journal of Interpersonal Violence*, 36(1-2). pp. 70-95.
- King, C. A., Horwitz, A., Berona, J., Jiang, Q. (2013) 'Acutely Suicidal Adolescents. Who Engage in Bullying Behavior: 1-Year Trajectories', *Journal of Adolescent Health*, 2013/53, pp. 43–50.
- Kircaburun, K., Jonason, P., Griffiths, M. D., Aslanargun, E., Emirtekin, E., Tosuntaş, Ş. B., Billieux, J. (2021) 'Childhood Emotional Abuse and Cyberbullying Perpetration: The Role of Dark Personality Traits', *Journal of Interpersonal Violence*, 36(21–22), pp. NP11877–NP11893.
- Kocsel, N. (2019) *A perszeveratív kogníciók pszichológiai és biológiai korrelátumai*. PhD értekezés, Budapest: ELTE
- König, A., Gollwitzer, M., Steffgen, G. (2010) 'Cyberbullying as an act of revenge?', *Australian Journal of Guidance and Counselling*, 20(2), pp. 210–224.
- Kulcsár, G. (2024) *Bullying és cyberbullying. Hogyan előzzük meg és kezeljük az iskolai és az online kortársbántalmazást?* Budapest: Novissima
- Kulcsár, G. (2022) 'Characteristics of Bullying and Cyberbullying and the State of Affairs of Anti-Bullying Efforts in Hungary', *Journal of Eastern European Criminal Law*, 2022/1, 31–41. o.
- Kulcsár, G. (2021) 'A digitális reziliencia jelentősége a cyberbullying elleni küzdelemben' in Nagy, M. (szerk.) *Gyerekekre fókuszálva: Konferenciakötet*. Pécs: PTE. pp. 136–145.
- Kulcsár, G. (2018) 'Összefüggések és dilemmák' in Menyhárd A., Varga I. (szerk.) *350 éves az Eötvös Loránd Tudományegyetem Állam- és Jogtudományi Kara: A jubileumi év konferenciasorozatának tanulmányai (I.-II. kötet)*. Budapest: ELTE Eötvös Kiadó. pp. 426–433.
- Kutatások a gyerekek közötti erőszakról [Online]. Available: <https://osztalyfonok.hu/344/> (Retrieved: 30 November 2024)
- Link, B. (2008) *Bewährungsstrafen: Schüler filmen Missbrauch auf Party*. Merkur, 15.06.2009. [Online]. Available: <https://www.merkur.de/lokales/regionen/bewaehrungsstrafen-schueler-filmen-missbrauch-party-355953.html> (Retrieved: 01 December 2024)

- Marciano, L., Schulz, P. J., Camerini, A.-L. (2020) 'Cyberbullying Perpetration and Victimization in Youth: A Meta-Analysis of Longitudinal Studies', *Journal of Computer-Mediated Communication*, 25(2), pp. 163–181.
- Murphy, C. M. (2024b) *Cyberbullying among young people: Laws and policies in selected Member States*. Brussels: EEPRS (EU)
- Murphy, C.M. (2024a) *Understanding cybercrime*. Brussels: EPRS (EU)
- Negreiro M. (2023) *Combating child sexual abuse online*. Brussels: EPRS (EU)
- Niestadt M. (2022) *The new European strategy for a better internet for kids (BIK+)*. Brussels: EPRS (EU)
- Reinhardt, M., Kökönyei, Gy., Drubina, B., Urbán, R. (2021) 'A nem szuicidális önsértés és motivációjának mérése serdülőknél: az állítások az önsértés kapcsán kérdőív (ISAS-HU) magyar adaptációja', *Magyar Pszichológiai Szemle*, 76(3-4) pp. 515–548.
- Ren, Q., Jiang, S. (2021) 'Acculturation Stress, Satisfaction, and Frustration of Basic Psychological Needs and Mental Health of Chinese Migrant Children: Perspective from Basic Psychological Needs Theory', *International Journal of Environmental Research and Public Health*, 18(9)
- Rassin, E., de Ross, M., van Dongen, J. (2024) 'Dark personality traits and deception, and the short dark tetrad (SD4) as integrity screening instrument', *Scientific Reports*, 14(1) pp. 311.
- Saha, K., Tech, G., Chandrasekharan, E., De Choudhury, M. (2019) 'Prevalence and Psychological Effects of Hateful Speech in Online College Communities' in Boldi, P., Foucault Welles, B. (eds.) *WebSci '19: Proceedings of the 10th ACM Conference on Web Science*. New York: Association for Computing Machinery. pp. 255–264.
- Schmid, U.K., Kümpel, A.S., Rieger, D. (2022) 'How social media users perceive different forms of online hate speech: A qualitative multi-method study', *New Media & Society*, pp. 1–19.
- Skilbred-Fjeld, S., Reme, S. E., Mossige, S. (2020) 'Cyberbullying involvement and mental health problems among late adolescents', *Cyberpsychology: Journal of Psychosocial Research on Cyberspace*, 14(1), pp. 1–16.
- Slonje, R., Smith, P. K., Frisén, A. (2013) 'The nature of cyberbullying, and strategies for prevention', *Computers in Human Behavior*, 29(1), pp. 26–32.
- Sorrentino, A., Baldry, A. C., Farrington, D. P., Blaya, C. (2019) 'Epidemiology of Cyberbullying across Europe: Differences between Countries and Genders', *Educational Sciences: Theory & Practice*, 19(2), pp. 74–91.
- Subrahmanyam, K., Greenfield, P. M. (2008) 'Online Communication and Adolescent Relationships', *Children and Electronic Media*, 18(1), pp. 119–203.

- Vannucci, A., Flannery, K. M., Ohannessian, C. M. (2017) 'Social media use and anxiety in emerging adults', *Journal of Affective Disorders*, 2017/207, pp. 163–166.
- Varela, J. J., Hernández, C., Miranda, R., Barlett, C. P. Rodríguez-Rivas, M. E. (2022) 'Victims of Cyberbullying: Feeling Loneliness and Depression among Youth and Adult Chileans during the Pandemic', *International Journal of Environmental Research and Public Health*, 19(10)
- Varjas, K., Talley, J., Meyers, J. Parris, L., Cutts, H. (2010) 'High school students' perceptions of motivations for cyberbullying: an exploratory study', *Western Journal of Emergency Medicine*, 11(3), pp. 269–273.
- Visionaries Project. New Forms of School Bullying and Violence. Cyberbullying, Happy Slapping and Other New Trends. International Online Conference, April 24 – May 19, 2006. Conference Report. VISIONARIES-NET project funded by the European Commission within the Socrates Minerva Program
- Wypych, M., Bilewicz, M. (2022) 'Psychological toll of hate speech: The role of acculturation stress in the effects of exposure to ethnic slurs on mental health among Ukrainian immigrants in Poland', *Cultural Diversity and Ethnic Minority Psychology*, DOI: 10.1037/cdp0000522
- Zhu, C., Huang, S., Evans, R., Zhang, W. (2021) 'Cyberbullying Among Adolescents and Children: A Comprehensive Review of the Global Situation, Risk Factors, and Preventive Measures', *Frontiers in Public Health (Section Public Mental Health)*, 2021/9, pp. 1–12.
- 1488/2016. (IX. 2.) Korm. határozat a Gyermekek számára biztonságos internetszolgáltatás megteremtéséről, a tudatos és értéktérítő internethasználatról és Magyarország Digitális Gyermekvédelmi Stratégiájáról (1488/2016 (IX. 2.) Government Decision on the Creation of a Safe Internet Service for Children, on the Conscious and Value-Creating Use of the Internet and on the Digital Child Protection Strategy of Hungary)

IV. ONLINE HATE SPEECH, CYBERBULLYING AND THE ECTHR: TOWARD A COMMON EUROPEAN STANDARD?

NÓRA BÉRES

1. Introduction

Keeping pace with the rapid advances of science and technology has become a constant challenge for modern legislation, and human rights law is no exception. That is also true for online hate speech and cyberbullying: a significant part of hate crime and bullying-type behaviour has moved to the internet, and the legislator needs to adapt or develop solutions to this relatively new context while taking into consideration the specifics of the online space as well as the traditional solutions applied to offline cases.

The development of science and technology poses a particularly difficult test for international law, mainly because of the absence of decentralised legislation, the significant differences in the will of States, the delays in the conclusion and ratification of treaties, the (excessively) general or vague content of the provisions adopted and the inherent uncertainties of customary law. At the same time, international human rights courts, which are in some respect at the forefront of international adjudication, cannot remain silent about the inertia of legislation in providing real protection to applicants seeking redress, and are therefore trying to catch up with the development of science and technology by using ‘creative tools’ of judicial interpretation. In this respect, the European Court of Human Rights (hereinafter: ECtHR or Court) is an indispensable point of reference, as the Court, by applying the

https://doi.org/10.47079/2025.kprhk.cyberb.4_5

doctrines of evolutionary interpretation¹ and inherent obligations², allows the European Convention on Human Rights³ (hereinafter: ECHR or Convention), adopted more than 70 years ago, to function as a living instrument to this day, offering effective protection to the 830 million people covered by the Convention.⁴

The ECtHR has a very rich case-law on online hate speech and cyberbullying, especially on the former, and this chapter aims to outline the human rights contours of these crimes and unlawful conducts through the Strasbourg case-law. This chapter thus examines the issue from the perspective of victims, while primarily applying a case-analysis methodology. The selection of cases has been primarily focused on those directly related to the online context, although some general but closely related findings need to be explored in order to present examples of offline hate speech and bullying type behaviour. As hate speech and bullying typically involve different human rights violations, they will be analysed in separate sections.

2. Online hate speech in the case-law of the ECtHR

2.1. General overview: hate speech in international law

Hate speech does not have a universal, stand-alone definition in international law, but the international community has adopted a number of human rights instruments over the past eight decades that are relevant to this issue. The Universal Declaration of Human Rights⁵ (hereinafter: UDHR) was the first inter-

¹ Bernhardt, 2009, pp. 11–25; Dzehtsiarou, 2011, pp. 1730–1745.

² For more detail see McBride, J. (2021) *The Doctrines and Methodology of Interpretation by the European Court of Human Rights on the European Court of Human Rights* [Online]. Available at: <https://rm.coe.int/echr-eng-the-doctrines-and-methodology-of-interpretation-of-the-europe/1680a20aee>

³ European Convention on Human Rights, opened for signature 4 November 1950, E.T.S. No. 005, entered into force 3 September 1953. More rights are granted by additional protocols to the Convention [Protocols 1 (E.T.S. No. 009), 4 (E.T.S. No. 046), 6 (E.T.S. No. 114), 7 (E.T.S. No. 117), 12 (E.T.S. No. 177), 13 (E.T.S. No. 187), 14 (C.E.T.S. No. 194), 15 (C.E.T.S. No. 213) and 16 (C.E.T.S. No. 214)].

⁴ Council of Europe, European Court of Human Rights, Annual Report of 2020 [Online]. Available at: https://www.echr.coe.int/Documents/Annual_report_2020_ENG.pdf

⁵ United Nations General Assembly Resolution 217 A (III) (A/RES/3/217) adopted on 10 December 1948.

national instrument of the 20th century to declare the freedom of expression.⁶ Among the treaties that have come into being under the auspices of the United Nations, one can cite the International Convention on the Elimination of All Forms of Racial Discrimination adopted in New York on 21 December 1965⁷ (hereinafter: ICERD). Art. 4⁸ of the ICERD imposes an obligation on its States Parties to criminalise conducts that promote racial or ethnic superiority or incite hatred. On the other hand, Art. 19 of the International Covenant on Civil and Political Rights⁹ (hereinafter: ICCPR) provides for the criminalisation of conducts that promote racial or ethnic superiority or incite hatred. Art. 19¹⁰ guarantees the freedom of expression, and Art. 20¹¹ prohibits war propaganda and incitement to hatred on national, racial or religious grounds. Among the universal soft law documents, the Human Rights Committee's General Comment

6 Art. 19 of the UDHR: *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

7 International Convention on the Elimination of All Forms of Racial Discrimination, New York, 7 March 1966, United Nations, Treaty Series, vol. 660, p. 195.

8 Art. 4 of the ICERD: *States Parties condemn all propaganda and all organizations which are based on ideas or theories of superiority of one race or group of persons of one colour or ethnic origin, or which attempt to justify or promote racial hatred and discrimination in any form, and undertake to adopt immediate and positive measures designed to eradicate all incitement to, or acts of, such discrimination and, to this end, with due regard to the principles embodied in the Universal Declaration of Human Rights and the rights expressly set forth in article 5 of this Convention, inter alia: (a) Shall declare an offence punishable by law all dissemination of ideas based on racial superiority or hatred, incitement to racial discrimination, as well as all acts of violence or incitement to such acts against any race or group of persons of another colour or ethnic origin, and also the provision of any assistance to racist activities, including the financing thereof; (b) Shall declare illegal and prohibit organizations, and also organized and all other propaganda activities, which promote and incite racial discrimination, and shall recognize participation in such organizations or activities as an offence punishable by law; (c) Shall not permit public authorities or public institutions, national or local, to promote or incite racial discrimination.*

9 International Covenant on Civil and Political Rights, New York, 16 December 1966, United Nations, Treaty Series, vol. 999, p. 171 and vol. 1057, p. 407.

10 Art. 19 of the ICCPR: *1. Everyone shall have the right to hold opinions without interference. 2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice. 3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.*

11 Art. 20 of the ICCPR: *1. Any propaganda for war shall be prohibited by law. 2. Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law.*

No. 34 on Art. 19 of the ICCPR¹² is a comprehensive interpretation of the freedom of expression, synthesising jurisprudence.

The definition of hate speech at the European level is much more concentrated, although most of its elements remain at the level of soft law. A recommendation of the Committee of Ministers of the Council of Europe¹³ marks,

“For the purposes of the application of these principles, the term ‘hate speech’ shall be understood as covering all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin”.

In addition, the European Commission against Racism and Intolerance of the Council of Europe's Recommendation¹⁴ uses the following definition,

“[Hate speech] means the use of one or more specific forms of expression – namely, the advocacy, promotion or incitement of the denigration, hatred or vilification of a person or group of persons, as well as harassment, insult, negative stereotyping, stigmatisation or threats against such a person or group of persons, as well as any form of expression – that is based on based on a non-exhaustive list of personal characteristics or status that includes ‘race’, colour, language, religion or belief, nationality or national or ethnic origin, as well as descent, age, disability, biological sex, social sex, gender identity and sexual orientation.”

In addition, it should be noted that the 2003 Supplementary Protocol to the 2001 Budapest Convention on Cybercrime against Xenophobia and Racism¹⁵ partially covers the elements of hate speech but does not address cases where hate is motivated by gender, sexual orientation or disability.¹⁶

¹² United Nations, International Covenant on Civil and Political Rights, Human Rights Committee 102nd session, Geneva, 11-29 July 2011, General Comment No. 34, Article 19: Freedoms of Opinion and Expression [Online]. Available at: <https://www2.ohchr.org/english/bodies/hrc/docs/gc34.pdf>

13 Committee of Ministers of the Council of Europe Recommendation No R 97(20) 30.10.1997 [Online]. Available at: <https://rm.coe.int/1680505d5b>

¹⁴ European Commission against Racism and Intolerance (ECRI), General Policy Recommendation No. 15 on “Hate Speech” 8.12.2016 [Online]. Available at: <https://rm.coe.int/ecri-general-policy-recommendation-no-15-on-combating-hate-speech/16808b5b01>

15 Additional Protocol to the Convention on Cybercrime, concerning the criminalisation
of acts of a racist and xenophobic nature committed through computer systems (ETS No.
189), 28 January 2003.

16 For more details on combating hate speech in the Council of Europe, see Council of Europe, Online Hate Speech [Online]. Available at: [https://www.coe.int/en/web/cyberviolence/online-hate-speech#%22103915149%22:\[0\],%22103915178%22:\[1\]](https://www.coe.int/en/web/cyberviolence/online-hate-speech#%22103915149%22:[0],%22103915178%22:[1])

The lack of a universal hard-law definition of hate speech leads to the practical consequence that the conduct and facts under which this act is committed vary widely from one state to another. However, a modest guideline can be confidently applied on the basis of American and European concepts of freedom of expression: if a communication creates a clear and present danger of violence,¹⁷ it will be considered hate speech.

2.2. Hate speech in Strasbourg case-law: a general framework

At the regional level, the most effective legal protection against hate speech is undoubtedly provided by the Strasbourg Court, which can rely on Article 10 of the ECHR on freedom of expression¹⁸ and Article 17 of the same convention on the prohibition of abuse of rights.¹⁹ As early as 1976, in *Handyside v. United Kingdom*,²⁰ in which the applicant was the owner of a British publishing house which had bought the exclusive rights to distribute in the UK a publication for teenagers containing sexually explicit contents which many considered obscene, but the distribution of the book was banned on grounds of public morality and many copies were confiscated, the Court found that in principle freedom of expression is an indispensable element of democratic societies and a fundamental condition for progress and the development of all human beings.²¹ Thus, Article 10(2) of the ECHR applies not only to ‘information’ and ‘ideas’ which are neutral or favourable in their reception or perception, but also to those which attack,

17 See Koltay, 2013, pp. 91–123. For the interpretation issues arising in Hungarian jurisprudence and the constitutional standards underlying the criminalisation of incitement against the community.

18 Article 10 (1) of the ECHR (Freedom of expression): *1. Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises. 2. The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*

19 Article 17 of the ECHR (Prohibition of abuse of rights): *Nothing in this Convention may be interpreted as implying for any State, group or person any right to engage in any activity or perform any act aimed at the destruction of any of the rights and freedoms set forth herein or at their limitation to a greater extent than is provided for in the Convention.*

20 *Handyside v. United Kingdom*, no. 5493/72, § 49, 7 December 1976.

21 On the two conflicting tests applied by the ECtHR in hate speech cases see Sottiaux, 2022, pp. 1193–1211.

shock or disturb the State or a part of the population.²² This stems from the requirements of pluralism, tolerance and openness, without which there will be no ‘democratic society’. It follows from the latter that any formality, condition, restriction or penalty applied in this area must be proportionate to the legitimate aim pursued. It is clear also from the judgment that freedom of expression is not limited to ‘pleasant’ communications but covers a much wider spectrum. Moreover, freedom of expression issues are most likely to come to the attention of the legislator when offensive, shocking or disturbing ideas, information, principles and views surface.²³

Freedom of expression therefore extends to criticism, satire, and even shocking, disturbing or offensive communications to certain sections of society, as these are the very embodiment of pluralism, tolerance and openness in a democratic society.²⁴ On the other hand, as will be seen below, offensive and seriously offensive internet communications which go beyond the limits of the satirical genre and even amount to defamation are no longer covered by Article 10 of the Convention.²⁵ As the ECtHR held in *Erbakan v. Turkey*,²⁶ where the applicant, a former Prime Minister and President of the Turkish Welfare Party, was sentenced to one year’s imprisonment and a fine for inciting the public to racial and religious hatred in a speech during the 1994 election campaign, tolerance and respect for the equal dignity of all human beings are the cornerstones of a democratic, pluralist society. Consequently, in certain democratic societies it may be necessary to sanction or even prevent any expression of opinion which spreads, incites, promotes or supports hatred based on intolerance provided that any formality, condition, restriction or penalty applied in this respect is proportionate to the legitimate aim pursued.

The ECtHR gives the Contracting Parties a margin of appreciation derived from the principle of subsidiarity,²⁷ however,²⁸ this margin is not unlimited, nor is it equal, given the diversity of opinions. Thus, e.g., in the case of online comments on politics, the freedom of expression of individuals is highly protected and the discretion of the State is reduced,²⁹ whereas, for example, in the

22 Mchangama – Alkiviadou, 2021, pp. 1008–1042.

23 Simon, 2018, p. 726.

24 *Perrin v. United Kingdom* (dec.), no. 5446/03, 18 October 2005.

25 *Bartnik v. Poland* (dec.), no. 53628/10, 11 March 2014.

26 *Erbakan v. Turkey*, no. 59405/00, § 56, 6 July 2006.

27 Vila, 2017, pp. 393–413.

28 The Strasbourg Court first elaborated the principle of freedom of discretion in detail in *Handyside v. United Kingdom*, cited above. See for more details.

29 See *Axel Springer AG v. Germany*, no. 39954/08, § 90, 7 February 2012; *Morice v. France*, no. 29369/10, § 125, 23 April 2015.

case of comments on commercial content, the public authorities may apply a wider range of restrictions.

The case of *Erbakan v. Turkey* illustrates a clear conclusion that can be drawn from the text of the Convention, namely that freedom of expression, although a human right of paramount importance, is not an absolute right: there are values that take precedence over it in certain cases and in certain social contexts. Article 10(2) of the ECHR enumerates possible grounds for restrictions that are acceptable in a democratic society, namely national security, territorial integrity, public safety, prevention of disorder or crime, protection of public health or morals, protection of the reputation or rights of others, prevention of the disclosure of confidential information, or the maintenance of the authority and impartiality of the judiciary. However, even these restrictions can only be applied if they are duly justified and restrictive.³⁰

States' obligations to protect institutions in relation to racism, hate speech, discrimination, intolerance, terrorism and the glorification of violence are particularly prominent in ECtHR case-law. For example, in *Jersild v. Denmark*,³¹ where the applicant was prosecuted for having interviewed three young people from the 'Greenjackets' group on a TV programme making racist remarks and inciting hatred, irrespective of the fact that the programme was a problem report on anti-immigration movements in a broader context, the European Commission of Human Rights (hereinafter: ECommHR) has stated in principle that it considers the fight against all forms and manifestations of racial discrimination to be of fundamental importance. In *Gündüz v. Turkey*,³² where the applicant, the leader of an Islamist sect, made a strong criticism of democracy in a television programme, the Court reiterated that tolerance and respect for the equal dignity of all human beings are the cornerstones of democratic and pluralist societies, and that sanctions for behaviour which promotes, incites, spreads or justifies hatred based on intolerance may therefore be considered necessary in a democratic society, provided that such sanctions are proportionate to the aim pursued. In the same case, the ECtHR also made it clear that freedom of expression does not apply to hate speech, and that this applies to any communication which is incompatible with the fundamental values protected by the Convention, in accordance with Article 17 of the ECHR on the prohibition of abuse of rights. This includes, according to ECtHR case-law, the denial of the Holocaust, the support for Nazi ideology, association of all

³⁰ Simon, 2018, p. 730.

³¹ *Jersild v. Denmark*, no. 15890/89, § 30, 23 September 1994.

³² *Gündüz v. Turkey*, no. 35071/97, §§ 40-41, 4 December 2003.

Muslims with serious terrorist acts, or specifically, that Jews are the source of all evil in Russia.³³

In cases where the Strasbourg Court is dealing with hate speech, the Convention offers two possible alternatives. The first is the application of Article 17³⁴ (prohibition of abuse of rights), which excludes from the protection afforded by the ECHR opinions that constitute hate speech and deny the fundamental values of the ECHR. For instance, in *Seurot v. Francei*,³⁵ where the applicant was a high school geography and history teacher who had published a violent, racist and hateful article in the school newspaper and was dismissed for it, the Court clarified the relationship between Article 10 and Article 17 establishing that Article 17 ECHR unquestionably excludes from the protection afforded by Article 10 any comment which constitutes an attack directly against the values enshrined in the Convention.

The function of Article 17 is twofold: on the one hand, it acts as an interpretative rule and, on the other, it is used as one of the exceptions to admissibility. The latter means that, if the ECtHR considers the application to be abusive, it falls outside the scope of the protection afforded by the other articles of the Convention and the merits of the application are no longer examined.³⁶ This categorical exclusion is aptly referred to in the scholarly discussions as the ‘guilt-lotline effect’,³⁷ which is applied primarily, but not exclusively, to clearly established historical facts.³⁸ The prohibition of abuse of rights was first invoked by the ECtHR in 1979 in *Glimmerveen and Hagenbeek v. the Netherlands*,³⁹ when it excluded the dissemination of ideas based on racial discrimination from the protection afforded by freedom of expression by invoking Article 17. A similar conclusion was reached by the ECtHR in *Kühnen v. Germany*⁴⁰ in relation to the reinstatement of the banned National Socialist German Workers’ Party, finding

33 See *Lehideux and Isorni v. France*, no. 55/1997/839/1045, §§ 46-58, 23 September 1998; *Garaudy v. France* (dec.), no. 65831/01, 7 July 2003; *Norwood v. United Kingdom* (dec.), no. 23131/03, 16 November 2004; *Witzsch v. Germany* (dec.), no. 7485/03, 13 December 2005; *Pavel Ivanov v. Russia* (dec.), no. 35222/04, 20 February 2007.

34 The other approach is to invoke the limitations allowed by Article 10(2) (freedom of expression), which the ECtHR adopts in cases where the opinion in question, although it may constitute hate speech, is less likely to destroy the fundamental values of the Convention. Its application will be discussed later in this chapter.

35 *Seurot v. France* (dec.), no. 57383/00, 18 May 2004.

36 Bodnár, 2021, pp. 378–379.

37 Derenčinović, 2021, p. 8; Nikouei-Zamani, 2019, p. 68; Lobba, 2015, pp. 241-242; Canie-Voorhoof, 2011, p. 58.

38 Keane, 2007, p. 651.

39 *Glimmerveen and Hagenbeek v. Netherlands*, nos. 8348/78 and 8406/78, § 11, 11 October 1979.

40 *Kühnen v. Germany* (dec.), no. 12194/86, 28 May 1986.

that Article 10 of the Convention could not be invoked contrary to Article 17. Holocaust denial also sits at the common intersection of Articles 10 and 17: the applicant in *Remer v. Germany*⁴¹ was convicted by German courts due to his publication distributed, which claimed that gas chambers never existed in the Nazi concentration camps. Interestingly, in the latter two cases, the ECtHR invoked both Article 10(2) and Article 17 in its judgments, but unlike in *Glimmerveen and Hagenbeek v. the Netherlands*, it based its decisions on freedom of expression and followed the prohibition of abuse of rights only as a guideline.

Despite hate speech being one of the classic and clear exceptions to freedom of expression, there is no uniform definition of it in Strasbourg case-law. This is clear from the case of *Féret v. Belgium*,⁴² where the applicant was the President of the Belgian National Front and also the editor-in-chief of the party's publications inciting racist and xenophobic hatred, discrimination and violence, in which the majority of the Presiding Chamber held that any statement promoting, disseminating or justifying hatred based on intolerance constituted hate speech. In contrast, the judges who wrote the dissenting opinion interpreted the concept of hate speech more narrowly and did not consider the conduct to have been committed, as the applicant had not claimed the superiority of any racial group by his derogatory statements against immigrants.⁴³

2.3. The specifics of online hate speech in Strasbourg case-law

The scope of freedom of expression extends to both offline and online communications: the ECtHR Grand Chamber in *Delfi AS v. Estonia*⁴⁴ made it categorically clear that the ECHR applies to communications on the internet, although the specificity of the latter means that some rules cannot be derogated from. The Strasbourg Court pointed out, on the one hand, that internet content and communications, compared to the printed press, present a greater risk of violation of human rights and freedoms, in particular the right to privacy.⁴⁵ In *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, where the applicant was the editor-in-chief of the Odessa regional newspaper *Pravoye Delo*, and who, for reasons of cost-effectiveness, had on several occasions republished articles from other press organs and internet news portals without checking the authenticity of the sources, found that the electronic network, which serves billions of users

41 *Remer v. Germany* (dec.), no. 25096/94, 19 August 1994.

42 *Féret v. Belgium*, no. 15615/07, § 64, 10 December 2009.

43 Uitz, 2021, p. 296.

44 *Delfi AS v. Estonia*, no. 64569/09, § 131, 16 June 2015.

45 *Delfi AS v. Estonia*, § 133.

worldwide, is not currently subject to the same rules and control mechanisms as the printed press and is unlikely ever to be so.⁴⁶

One should also devote some attention at this point to *Delfi AS v. Estonia*, a landmark case,⁴⁷ where the ECtHR examined the liability of an internet news portal provider for comments posted anonymously by users of the site, requires more detailed analysis. The applicant, the Delfi AS, was one of the leading online content providers in the Baltic region, and operated an internet news portal where readers could post comments on online news items after entering a nickname, and some of them posted comments on the site that were clearly a serious violation of privacy rights. The applicant referred the case to the ECtHR, claiming that the national courts had found him liable because users had posted offensive comments about a ferry company under an online news item. At the request of the shipping company's legal representative, Delfi AS removed the comments some six weeks after they had been published. The clearly unlawful comments undoubtedly infringed the rights of others, so the question in the case was not whether the removal of the comments violated the users' right to freedom of expression, but whether holding Delfi AS liable for the comments posted by third parties violated the news portal's right to information.

In the respecting case, the Court ruled that an internet content provider can be held liable for user comments on its website. However, two clarifications should be added here. The first is that the case concerned a news portal operated on a professional basis for commercial purposes, where users were allowed to comment, even anonymously, on articles written by the site's editors. The ECtHR pointed out that the findings of the judgment did not apply to other types of websites, such as advertising, chat rooms or social networking sites. The second is that the comments by readers on the news portal were a serious violation of the privacy rights of others and constituted hate speech.

In its judgment, the Grand Chamber took the view that the recognition of the differences between internet content providers and traditional publishers is in line with international standards in this area, which tend to distinguish between the legal norms governing the activities of traditional print media and audiovisual media, as well as online media.⁴⁸ In its Recommendation to

46 *Editorial Board of Pravoye Delo and Shtetel v. Ukraine*, no. 33014/05, § 63, 5 May 2011.

47 For more details, see Nádori P. (2013) *Delfi AS v. Estonia: Strasbourg ruling on service provider liability for anonymous comments* [Online]. Available at: <https://www.researchgate.net/publication/272823952>.

48 *Delfi AS v. Estonia*, § 113.

Council of Europe Member States on the new definition of media,⁴⁹ the Committee of Ministers calls this a ‘differentiated and graduated’ approach, requiring that all service providers enjoy an appropriate form (differentiated) and level (graduated) of protection and that their responsibilities are also determined in accordance with Article 10 ECHR and other relevant standards developed by the Council of Europe. Therefore, the Grand Chamber considered that, given the specific nature of the internet, the ‘obligation and responsibility’ imposed on online news portals under Article 10 may differ to some extent from that of traditional publishers as regards third-party content.

The Court also buttressed in its judgment in *Delfi AS v. Estonia* that a professional online content provider should be aware of the relevant legislation and case-law, as it has easy access to legal advice, and that it was in a position to weigh the risks inherent in its activities and foresee their consequences within a reasonable time, and that therefore the restriction under Article 10(2) of the Convention was ‘prescribed by law’.⁵⁰

In summary, in *Delfi AS v. Estonia*, the Grand Chamber laid down four criteria in relation to the liability of an internet content provider for comments posted by third parties: (i) the comments were offensive to human dignity, clearly unlawful and extreme in nature; (ii) the comments were posted under self-published articles of a commercially run internet content provider where the content provider explicitly encouraged its readers to post comments; (iii) the applicant had taken insufficient measures to remove the seriously offensive comments without delay (they were taken down only six weeks after their publication at the request of the victim); and (iv) the applicant was subject to a light sanction (320 EUR).

In this case, the ECtHR found no violation of Article 10 and agreed with the Estonian courts that the applicant was liable and that the restrictions on freedom of expression were not disproportionate. The ECtHR thus for the first time held a service provider liable for comments posted by third parties. Furthermore, the Court reiterated that comments which constitute hate speech are not protected by Article 10 of the Convention, i.e., they are not covered by the freedom of expression.

The Court pointed out on other occasions that the internet provides an unparalleled platform for freedom of expression, with the possibility for users

49 Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, HDS.IO/0008/13, 13 May 2013 [Online]. Available at: <https://edoc.coe.int/en/media/8019-recommendation-cmrec20117-on-a-new-notion-of-media.html>.

50 *Delfi AS v. Estonia*, § 129.

to share their communications easily, even anonymously.⁵¹ However, this advantage can be accompanied by certain dangers: defamatory and other types of clearly illegal speech, including incitement to violence and hate speech, can spread around the world in seconds, at speeds previously unimaginable, and remain permanently available on the internet with a few clicks. As the rights under Articles 8 and 10 of the Convention deserve equal respect, a balance must be struck between them that preserves the essence of both the right to privacy and freedom of expression. In line with this, while the use of the internet brings non-negligible benefits to the exercise of freedom of expression, liability for defamation, other unlawful communications and hate speech remains, and States Parties to the ECHR must ensure effective legal protection for violations of privacy rights in such cases as well.

Another lesson can be learnt from the case of *Hungarian Content Providers Association and Index.hu Zrt. v. Hungary*,⁵² which concerned the liability of the self-regulatory body of internet content providers and the internet news portal Index.hu for vulgar and offensive comments posted by users on their websites after they published an opinion criticising the deceptive business practices of two real estate websites. The defendants challenged the Hungarian court judgments against them, which effectively ordered them to moderate the content of comments posted by readers on their websites, arguing that this was contrary to freedom of expression. The ECtHR did indeed find a violation of the Convention in the case. Although they are not the publishers of the comments, online news portals have a duty and a responsibility for the content on their sites. The Court nevertheless held that the Hungarian courts, in deciding whether the applicants were liable, had not properly balanced the competing fundamental rights, namely the applicants' right to freedom of expression and the right of the real estate websites to respect their business reputation (the Hungarian courts had taken the illegality of the comments as a given, as they had damaged the business reputation of the real estate websites).

At this point, it is necessary to point out the essential difference between the *Delfi AS v. Estonia* case and the *Hungarian Content Providers Association and Index.hu Zrt. v. Hungary* case, given that at first glance, it can be seen that the ECtHR in the former case held the provider liable for offensive and vulgar comments posted by users, while in the latter it ruled the opposite. The reason for this

51 *Delfi AS v. Estonia*, § 110; *Ahmet Yıldırım v. Turkey*, no. 3111/10, § 48, 18 December 2012; *Times Newspapers Ltd v. United Kingdom* (nos. 1 and 2), nos. 3002/03 and 23676/03, § 27, 10 March 2009.

52 *Hungarian Content Providers Association and Index.hu Zrt. v. Hungary*, no. 22947/13, § 29-91, 2 February 2016.

difference is that the ‘Hungarian case’ did not contain the key element of the ‘Estonian case’, namely hate speech and incitement to violence: although the comments involved in the case of *Hungarian Content Providers Association and Index.hu Zrt. v. Hungary* were offensive and vulgar, the comments did not clearly constitute unlawful speech.

A similar conclusion can be drawn from the case of *Pihl v. Sweden*,⁵³ where the Court declared the application manifestly ill-founded and therefore inadmissible. The applicant was the victim of a defamatory comment published anonymously by a third party on an internet blog, who brought a civil action against the provider of the website, a small non-profit association, asking the court to declare the defendant liable for the offensive anonymous comments. After his action was dismissed by the Swedish courts, the applicant applied to the ECtHR for a declaration that his right to reputation and right to privacy had been violated. The ECtHR has highlighted the need to strike a delicate balance between the applicant’s right to privacy and the website provider’s freedom of expression in cases such as this, and the Swedish courts have done so in this case. The Court reiterated the importance it attached to the fact that, although the comment was offensive, it did not constitute hate speech or incitement to violence, it also based its finding of no breach on the fact that the blog provider was a small non-profit association, that the provider removed the offending post the day after the applicant’s comment, and that the comment had been on the website for only nine days.

In *Smajić v. Bosnia and Herzegovina*,⁵⁴ where the applicant was convicted by the national courts for incitement to national, ethnic and religious hatred, antagonism and intolerance after he had detailed in a series of internet posts what military measures would be necessary in the Serb-populated villages of the Brčko District in the event of another South Slav war. The ECtHR found no violation of Article 10 and declared the complainant’s application manifestly unfounded. The Court confirmed that the national criminal court had given adequate reasons for its decision, namely that the accused had used seriously offensive language against Serbs, touching on a very sensitive point of ethnic issues in post-conflict Bosnian society.

In *Nix v. Germany*,⁵⁵ the applicant was convicted for posting a picture of former Nazi leader Heinrich Himmler and a swastika on a blog. In the proceedings, the defendant complained that the German courts had failed to take into account, when handing down the judgment, that the purpose of his post

⁵³ *Pihl v. Sweden*, no. 74742/14, §§ 22-38, 17 February 2017.

⁵⁴ *Smajić v. Bosnia and Herzegovina*, no. 48657/16, §§ 29-42, 8 February 2018.

⁵⁵ *Nix v. Germany* (dec.), no. 35285/16, 5 April 2018.

was to protest against discrimination against immigrants in education and the workplace and that the decision therefore infringed his right to freedom of expression. Despite the ECtHR's recognition that the applicant's purpose in publishing the image was not indeed to disseminate totalitarian propaganda or incite hatred, and that the applicant may have intended to contribute to a public debate of public interest, the Court found that the applicant had resorted to a kind of 'communication taboo' to attract attention, which is not protected by Article 10 of the ECHR.

The petitioner in the case *Savva Terentyev v. Russia*⁵⁶ was convicted of inciting hatred after posting insulting comments about police officers under a blog post. The ECtHR found a violation of Article 10 of the Convention, confirming that although the comments posted by the applicant were indeed offensive and shocking, this alone did not constitute grounds for interfering with the State's freedom of expression.

In *Kilin v. Russia*,⁵⁷ the national authorities prosecuted the applicant for dissemination of extremist content and sentenced him to 18 months suspended imprisonment and a probation period of the same duration. According to the prosecution, the applicant had posted video and audio recordings with racist content of neo-Nazis, the use of racial epithets, persons of apparent Caucasian origin and calls for extremism on a popular online community site. In the present case, the Court held that the applicant's prosecution was contrary to Article 10 of the Convention. Likewise, the ECtHR ruled that the applicant had not infringed Article 10 of the ECHR: taking into account the racist nature of the material and the fact that the applicant did not, when publishing the content, attach any mitigating circumstances to the content, namely that it was satirical work of art, the national authorities had established conclusively that the material complained of incited ethnic hatred and that the applicant had a clear intention to incite acts of hatred or intolerance.

*Standard Verlagsgesellschaft mbH v. Austria*⁵⁸ focused on a court order against the applicant media company, which ordered the publication of a list of registered commentators on the website of the daily newspaper *Der Standard*, following the publication of a number of comments on the website which linked politicians, including neo-Nazis. Although the comments were removed by the applicant, it refused to disclose the identity of the users who had written them. In the case, the ECtHR found the injunction to be in breach of the Convention, arguing that the national authorities had generally failed to comply with their

⁵⁶ *Savva Terentyev v. Russia*, no. 10692/09, §§ 41-87, 28 August 2018.

⁵⁷ *Kilin v. Russia*, no. 10271/12, §§ 44-96, 15 May 2021.

⁵⁸ *Standard Verlagsgesellschaft mbH v. Austria* (no. 3), no. 39378/15, §§ 49-97, 7 December 2021.

duty to balance the fundamental rights at stake and had not provided adequate reasoning to justify the interference with the rights of the complainant media company. The Court found that the comments at issue in the case did not constitute hate speech or incitement to violence, they were merely part of a political debate of public interest, and that the restriction on freedom of expression was therefore not necessary in a democratic society.

In *Sanchez v. France*,⁵⁹ which was referred to the Grand Chamber on 17 January 2022, the applicant was convicted of incitement against a religious group. The applicant was a local candidate standing in the parliamentary elections who failed to promptly delete hateful comments posted by others on his Facebook site. The ECtHR Chamber of seven judges ruled by 6 to 1 that the applicant's criminal conviction did not infringe freedom of expression: the French criminal court's judgment was properly reasoned and within the margin of appreciation granted to Contracting Parties in accordance with the principle of subsidiarity, and the restriction was necessary in a democratic society. Thus, with regard to user comments on the internet that contain hate speech or direct incitement to violence, the obligations arising from Article 10(2) of the ECHR can be established for internet news portals that allow the publication of reader comments on their websites for commercial and professional purposes.⁶⁰

In addition, the ECtHR has also held that certain statements, without directly constituting an incitement to hatred, can be just as serious and harmful and are therefore incompatible with the Convention. A striking example of this is *Vejdeland v. Sweden*,⁶¹ where the Court held that discrimination based on sexual orientation is as serious as discrimination based on race, descent or colour. In this context, particular vigilance is needed in the online space, where a debate on a legitimate issue can easily escalate into a debate on a legitimate issue, and discriminatory remarks can be made that violate the Convention, and that may harm the human rights and dignity and reputation of minorities or vulnerable groups. Given that the line between legality and illegality is extremely thin, comments by internet users require particular vigilance on the part of law enforcement, even if the original intention of the commentators was not to express contempt for individuals or groups.

⁵⁹ *Sanchez v. France* (dec.), no. 45581/15, 2 September 2021.

⁶⁰ For a detailed analysis see Kupsch, F. (2021) 'Watch Your Facebook Comment Section! Holding Politicians Criminal Liable for Third Parties' Hate Speech – No Violation of Freedom of Expression under the ECHR' *Völkerrechtsblog* [Online]. Available at: <https://voelkerrechtsblog.org/watch-your-facebook-comment-section/>.

⁶¹ *Vejdeland and others v. Sweden*, no. 1813/07, §§ 55-57, 9 February 2012.

3. Cyberbullying in the case-law of the ECtHR

A study of the Council of Europe,⁶² published in December 2021, pointed out that the curfew, restrictions and closures imposed by the COVID-19 pandemic had increased the amount of time spent online, making already vulnerable groups, especially women and children, more vulnerable to cybercrime.⁶³ Although numerous Council of Europe conventions regulate certain forms of cyberbullying, which has become particularly acute in recent years, and provide some solutions to this problem, such as the 2001 Budapest Convention on Cybercrime,⁶⁴ the 2007 Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse,⁶⁵ or the 2011 Lanzarote Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, the Istanbul Convention on combating and preventing violence against women and violence in relationships,⁶⁶ it can be established that the ECHR is the most effective regional human rights instrument in force on the old continent, as it is accompanied by judicial protection and the implementation of the Strasbourg Court's judgments is monitored by the Committee of Ministers of the Council of Europe.

Therefore, as with online hate speech, this section attempts to provide a comprehensive overview of the human rights aspects of cyberbullying by reviewing the relevant ECtHR case-law. Accepting the criminological position⁶⁷ that bullying or cyberbullying is an umbrella term, difficult to define and can take many forms, this diversity is demonstrated by the respecting cases selected from the case-law of the Court. In addition, the presentation of case-law seems appropriate because of the importance of judicial interpretation, not only at national but also at international level, given the technical novelty of historical facts.

62 Van der Wilk, E. (2021) *Protecting Woman and Girls from Violence in the Digital Age. The Relevance of the Istanbul Convention and the Budapest Convention on Cybercrime in Addressing Online and Technology-Facilitated Violence against Women* [Online]. Available at: <https://rm.coe.int/prems-153621-gbr-2574-study-online-a4-bat-web/1680a4cc44>

63 The study also provides a detailed analysis of which provisions of the Budapest Convention and the Istanbul Convention can provide protection in cases of cyberbullying of women and girls.

64 Act LXXIX of 2004 on the proclamation of the Council of Europe Convention on Cybercrime, signed in Budapest on 23 November 2001.

65 Act XCII of 2015 on the proclamation of the Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse and on the amendment of certain acts in this context.

66 Council of Europe Convention on preventing and combating violence against women and domestic violence (CETS No. 210), 11 May 2011.

67 Parti, 2016, pp. 115–117.

As it will be seen later, bullying-type acts are characterised by the fact that they are primarily brought before the Strasbourg Court because of the violation of the right to privacy. The general truth that the rise of the information society has made the protection of privacy one of the greatest challenges of the modern age is, of course, also true of the ECtHR.⁶⁸ The right to respect for private and family life, which includes respect for home and correspondence, is found in Article 8 of the ECHR,⁶⁹ and it is no exaggeration to say that it is certainly the least definable provision of the Convention.⁷⁰ The right to privacy, as a classic first-generation human right, requires both abstention and non-action on the part of the State, and also entails an obligation to protect institutions, i.e., the State must create in the national legal system the legal guarantees that provide adequate protection for the private sphere of the individual. The right to privacy, like freedom of expression, is not an absolute human right and ECHR Contracting States do not enjoy a permanent margin of appreciation in restricting it. Generally speaking, the more sensitive the right protected, or the more relevant it is to the identity and privacy of the individual, the narrower the margin of appreciation granted to the State.⁷¹

In the same vein, the ECtHR thus also imposes a positive obligation on States Parties to the Convention in the fight against online violence and cybercrime, and this obligation is even more pronounced in the case of vulnerable groups. The Court has declared various social groups vulnerable in a number of judgments, with the practical consequence of a stricter obligation on the part of the State to protect its institutions.

It is clear from the case-law of the ECtHR that the rights of children and young people, given their physical and mental vulnerability, must be protected in all circumstances, as they can access information on the internet with unprecedented ease and speed and can easily be targeted for sexual abuse or even paedophilia.

The latter is perfectly illustrated in *K.U. v. Finland*,⁷² where a 12-year-old boy was the victim of an anonymous stranger who placed an advertisement with

⁶⁸ Balogh, 2018, p. 470.

⁶⁹ Article 8 of the ECHR: (1) *Everyone has the right to respect for his private and family life, his home and his correspondence.* (2) *An authority may intervene in the exercise of this right only in cases provided for by law, where it is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of public health or morals, or for the protection of the rights and freedoms of others.*

⁷⁰ Harris et al., 2018, p. 522.

⁷¹ Sulyok, 2021, pp. 183–184.

⁷² *K.U. v. Finland*, no. 2872/02, § 43, 2 December 2008.

sexual content on his behalf on an online dating site. The child's father was unable to bring criminal proceedings against the perpetrator in Finland because, under the laws in force at the time, the investigating authorities could not require the service provider to identify the person who had shared the advertisement. The Court found that the State had failed to fulfil its positive obligation to ensure that the child's right to privacy was adequately protected and that the child's physical and mental health was not protected against the obligation of confidentiality. The ECHR protects physical and mental integrity under Article 8 and, in this light, anonymity on the internet and the obligation of confidentiality should not prevent the State from protecting the rights of potential victims, especially when it comes to a vulnerable group. The obligation of confidentiality cannot be absolute, and the legislator must provide an appropriate framework to reconcile the different competing needs for protection.

In *Muscio v. Italy*,⁷³ the president of an association of Catholic parents received pornographic e-mails from an unidentified sender, but his claim against the unknown person was rejected by the national courts after he tried to seek redress through the courts. Although the ECtHR has ruled that unsolicited content received electronically may constitute an interference with the right to privacy, by registering for an e-mail account, users of e-mail services acknowledge that their privacy cannot be absolutely protected on the internet and that they are exposed to the risk of unwanted messages, which the use of various filters can otherwise address. Given that the case in Italy was not unique and that many other States have also encountered objective difficulties in combating anonymous spam senders, modern technical means are not always sufficient to identify the sender, the Court did not confirm that the State was required to make additional efforts to comply with its obligation to protect institutions.

In *Buturugă v. Romania*,⁷⁴ the applicant was a victim of domestic violence: her husband not only abused her physically and threatened her with death, but after the parties divorced, he hacked into her electronic accounts, including her Facebook profile, and then downloaded her private conversations, documents and photos. The ex-wife made several attempts to seek help from the Romanian authorities, first for physical abuse and then for threats to withdraw the complaint. Later, she requested a search of her electronic devices and initiated criminal proceedings on suspicion of mail fraud. The prosecutor's office did not investigate the death threats for lack of criminality and closed the case for

⁷³ *Muscio v. Italy* (dec.), no. 31358/03, 13 November 2007.

⁷⁴ *Buturugă v. Romania*, no. 56867/15, §§ 43-79, 10 February 2020.

breach of confidentiality, citing the lateness of the complaint and the lack of a link to domestic violence. The offender was eventually fined 250 EUR for other offences. The applicant appealed against the decision of the prosecution to the court, which issued a restraining order against the accused, but the ex-husband did not comply with the terms of the order and the police did not monitor its execution. In its judgment, the ECtHR made it clear that cyberbullying is a form of violence against women and girls and can take many forms, such as accessing the victim's computer, downloading personal data, sharing and manipulating data and photographs. In cases of domestic violence, cyber-surveillance is often used by the perpetrator. The Court also ruled that a breach of confidentiality of correspondence should have been taken into account in the investigation of domestic violence.⁷⁵

The applicant in *Volodina v. Russia*⁷⁶ was physically abused and harassed online by her former partner. The perpetrator created fake profiles on various social networking sites with the applicant's name, personal details and nude photos of her, and then introduced her classmates and teachers as acquaintances. He also hid a GPS tracker in the lining of the complainant's bag and sent her death threats in the form of electronic messages. The Russian authorities were initially reluctant to investigate the case, claiming lack of jurisdiction, and the investigation was closed two and a half years later, having been closed due to the statute of limitations. (The GPS tracker and the death threats were never investigated in the absence of a criminal offence.) In this case, the Court categorically highlighted that Contracted Parties to the Convention must take effective action against all forms of domestic violence, whether offline or online. Furthermore, the ECtHR also stated that, since cyberbullying is primarily a violation of the victim's right to privacy, criminal and civil law at national level is necessary to ensure that privacy is adequately protected. In its judgment, the Strasbourg Court found that Russia had breached its obligations to protect the institutions under the Convention by failing to provide adequate criminal law to prevent prosecution for cyber intimidation.⁷⁷

In *Tamiz v. United Kingdom*,⁷⁸ the applicant had complained to the Court that his reputation had been damaged by comments on a blog, the ECtHR found, in the context of the internet that the test of gravity of the infringement was of

⁷⁵ For more details see Sulyok M. (2021) *A thousand faces of abuse? Legal approaches from harassment to cyberbullying* [Online]. Available at: <https://jogaszegylet.hu/jogelet/a-bantalmazas-ezer-arca-jogi-megkozelitesek-a-zaklatastol-a-cyberbullyingig/>

⁷⁶ *Volodina v. Russia* (no. 2), no. 40419/19, §§ 33-68, 14 September 2021.

⁷⁷ For more details see McQuigg, 2021, pp. 155-167.

⁷⁸ *Tamiz v. United Kingdom*, no. 3877/14, §§ 80-81, 19 September 2017.

the utmost importance, as millions of users post offensive or even defamatory comments every day. However, these comments are mostly trivial in nature and reach such a narrow audience that they cannot actually harm the reputation of the victim. In this case, although the comments complained of were indeed vulgar and abusive, they did not go beyond the vulgar and degrading nature which is part of the normal style of communication on many internet portals.

By contrast, the facts of *Egill Einarsson v. Iceland*⁷⁹ met the test of gravity of the infringement. The petitioner was a well-known Icelandic blogger, writer and television figure who was prosecuted on suspicion of sexual assault, but the investigation was dropped for lack of evidence. Subsequently, the applicant consistently denied the crimes in an interview with a local magazine, which included a photograph of him on its front page. On the same day, someone altered the cover page photo and uploaded a picture on Instagram in which he accused her of committing sexual offences in vulgar language, called her a rapist and wrote the word ‘loser’ around her face. The Court’s examination focused on the question of whether the vulgar communication constituted a value judgment or a statement of fact in the present case. The ECtHR held that such a remark was capable of constituting an interference with the applicant’s private life if it reached a certain degree of seriousness. Furthermore, the Court pointed out that Article 8 should be interpreted as meaning that even if their conduct and public comments have provoked heated debate, public figures should not be required to tolerate being publicly accused of violent crimes without such statements being supported by facts. Another aspect of the case *Egill Einarsson v. Iceland*⁸⁰ was examined by the Strasbourg Court in a separate procedure. The Icelandic courts declared the defamatory comments about the applicant on Facebook to be null and void but refused to award him additional damages in the circumstances of the case. In the light of the ECtHR’s findings in the present case, the failure to award damages does not in itself amount to a violation of Article 8. In considering whether the applicant’s reputation was sufficiently protected, the ECtHR took into account, inter alia, the fact that the statements were published as comments on a Facebook page among hundreds or thousands of other comments and that they were promptly removed by their author at the applicant’s request.

⁷⁹ *Egill Einarsson v. Iceland*, no. 24703/15, § 52, 7 November 2017.

⁸⁰ *Egill Einarsson v. Iceland* (no. 2), no. 31221/15, §§ 38-39, 17 July 2018.

Summary

Both online hate speech and cyberbullying have strong human rights roots, but while the former mostly violates Article 10 on freedom of expression and Article 17 on the prohibition of abuse of rights, the latter regularly conflicts with Article 8 of the ECHR, the right to respect for private life. The Court's case-law also demonstrates that while hate speech case-law dates back several decades and the number of relevant cases is quite high, cyberbullying has only come to the attention of the ECtHR in recent years and the number of cases remains relatively low. Both hate speech and cyberbullying have no uniform definition in international law or in the case-law of the Strasbourg Court. The fragmented nature of the definition of hate speech is illustrated by the case of *Féret v. Belgium*, where the majority opinion of the presiding chamber of judges described as hate speech any statement based on intolerance that advocated, propagated or justified hatred, whereas the judges who delivered the dissenting opinion considered the superiority of racial groups to be an intrinsic part of the concept. Moreover, the definition of cyberbullying is not even present in the Strasbourg case-law, and the Court itself has only used the term once in the case of *Buturugă v. Romania*, stating that cyberbullying is a form of violence against women and girls.

Hate speech, despite the fact that freedom of expression extends not only to 'pleasant' communications, but also to criticism, satire, or even shocking, disturbing, offensive expressions, does not fall within the scope of the protection guaranteed by Article 10 of the Convention: the restriction of hate speech based on intolerance is considered necessary in a democratic society. Moreover, in cases where the facts are contrary to the fundamental values of democratic societies, such as Holocaust denial or support for Nazi ideology, the Strasbourg Court rejects applications submitted to it at the admissibility stage on the grounds of the prohibition of abuse of rights.

As far as the ECtHR's jurisprudence on online hate speech is concerned, *Delfi AS v. Estonia* is a significant milestone, as it was the first case in which the Strasbourg Court examined the liability of an internet news portal provider for comments posted anonymously by users of the site. The Grand Chamber based its findings of liability on the extreme, extremist, hate speech quality of the comments, as well as on the commercially run internet content provider's encouragement of commenting and its inadequate measures (i.e., the late removal of illegal comments). The standard of liability for the removal of anonymous comments posted by third parties is clearly established when the *Delfi AS v. Estonia* case is compared with the *Hungarian Content Providers Association and Index. hu Zrt. v. Hungary* case. There seems to be a contrast between the two cases

in that the ECtHR in the former held the service provider liable for offensive and vulgar comments posted by users, while in the latter it ruled the opposite. The reason for this is to be found in the dividing line between hate speech and offensive speech that is not clearly unlawful: although the comments in *Hungarian Content Providers Association and Index.hu Zrt. v. Hungary* were offensive and vulgar, unlike in *Delfi AS v. Estonia*, where the comments did not constitute clearly unlawful speech.

As for the umbrella terminology of cyberbullying, it can be mainly associated with cases of sexual harassment, intimate partner violence and defamation of reputation from ECtHR case-law. Consequently, it can be established that the Contracting Parties to the Convention have a particularly strong institutional obligation to protect the most typical victims of cyberbullying, namely women and children, and that this positive obligation extends to the creation of the necessary criminal law offences. On the other hand, the Strasbourg Court has also held that there may be situations where even modern technical means are not sufficient to identify the senders of spam and the complainant must tolerate a violation of his right to privacy because of unsolicited e-mails. Similarly, in the context of cyberbullying, the Court has ruled that the infringement must reach a certain level of seriousness, and that this level of seriousness must exceed the level of the degrading and vulgar comments posted by millions of people every day.

All in all, human rights of individuals are protected online and offline in the same way, only the specificities of the internet can cause difference. This chapter has attempted to highlight these specificities by outlining the relevant case-law of the Strasbourg Court, with the expectation that the ECtHR will further enrich and refine the relevant details in the future.

Bibliography

- Balogh Cs. T. (2018) 'A magánélethez való jog' in Lamm V. (ed.) *Emberi Jogi Enciklopédia*. HVG-ORAC Lap- és Könyvkiadó Kft., pp. 470–475.
- Bernhardt, R. (2009) 'Evolutive Treaty Interpretation, Especially of the European Convention on Human Rights Focus Section: The Law of International Treaties in the 21st Century', *German Yearbook of International Law*, 42(1), pp. 11–25.
- Bodnár E. (2021) 'A joggal való visszaélés tilalma' in Sonnevend P., Bodnár E. (eds.) *Az Emberi Jogok Európai Egyezményének kommentárja*. HVG-ORAC Lap- és Könyvkiadó Kft., pp. 377–379.
- Cannie, H., Voorhoof, D. (2011) 'The Abuse Clause and Freedom of Expression in the European Human Rights Convention: An Added Value for Democracy and Human Rights Protection?' *Netherlands Quarterly of Human Rights*, 29(1), pp. 54–83.
- Derenčinović, D. (2021) 'Freedom of Expression and Its Restrictions in Europe – On the Applicability of Article 17 of The European Convention of Human Rights to Disinformation (Fake News)', *Law, Identity and Values*, 1(2), pp. 7–18.
- Dzehtsiarou, K. (2011) 'European Consensus and the Evolutive Interpretation of the European Convention on Human Rights' *German Law Journal*, 12(10), pp. 1730–1745.
- Harris, D., Bates, E., Buckley, C. (2018) *Harris, O'Boyle, and Warbrick: Law of the European Convention on Human Rights*. 4th Oxford: Oxford University Press.
- Keane, D. (2007) 'Attacking Hate Speech under Article 17 of the European Convention on Human Rights', *Netherlands Quarterly of Human Rights*, 25(4), pp. 641–663.
- Koltay, A. (2013) 'A nagy amagyar gyűlöletbeszéd-vita: a „gyűlöletre uszítás” alkotmányos mércéjének azonosítása felé', *Állam- és Jogtudomány*, 54(1-2), pp. 91–123.
- Lobba, P. (2015) 'Holocaust Denial before the European Court of Human Rights: evolution of an exceptional regime', *European Journal of International Law*, 26(1), pp. 237–253.
- Mchangama, J., Alkiviadou, N. (2021) 'Hate Speech and the European Court of Human Rights: Whatever Happened to the Right to Offend, Shock or Disturb?', *Human Rights Law Review*, 21(4), pp. 1008–1042.
- McQuigg, R. J. A. (2021) 'The European Court of Human Rights and Domestic Violence: Volodina v. Russia', *International Human Rights Law Review*, 10(1), pp. 155–167.
- Nikouei, M., Zamani, M. (2019) 'Jurisprudence of Tolerance: Hate Speech, Article 17 and Theory of Democracy in the European Convention on Human Rights', *International Human Rights Law Review*, 8(1), pp. 67–88.

- Parti K. (2016) 'A megfélemlítés (bullying) szabályozása Magyarországon és külföldön', *In Medias Res*, 5(1) pp. 114–146.
- Polgári E. (2017) 'A tagállamoknak biztosított mérlegelési szabadság doktrínája az Emberi Jogok Európai Bíróságának gyakorlatában', *Állam- és Jogtudomány*, 58(4), pp. 41–53.
- Simon É. (2018) 'A véleménynyilvánítás szabadsága' in Lamm V. (ed.) *Emberi Jogi Inciklopédia*. HVG-ORAC Lap- és Könyvkiadó Kft., pp. 726–734.
- Sottiaux, S. (2022) 'Conflicting Conceptions of Hate Speech in the ECtHR's Case Law', *German Law Journal* 23(9) pp. 1193–1211.
- Sulyok K. (2021) 'A magán és családi élethez való jog' in Sonnevend P., Bodnár E. (eds.) *Az Emberi Jogok Európai Egyezményének kommentárja*. HVG-ORAC Lap- és Könyvkiadó Kft., pp. 182–217.
- Uitz R. (2021) 'A véleménynyilvánítás szabadsága' in Sonnevend P., Bodnár E. (eds.) *Az Emberi Jogok Európai Egyezményének kommentárja*. HVG-ORAC Lap- és Könyvkiadó Kft., pp. 244–296.
- Vila, M. I. (2017) 'Subsidiarity, Margin of Appreciation and International Adjudication within a Cooperative Conception of Human Rights', *International Journal of Constitutional Law*, 15(2), pp. 393–413.

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. Szajbely, 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.

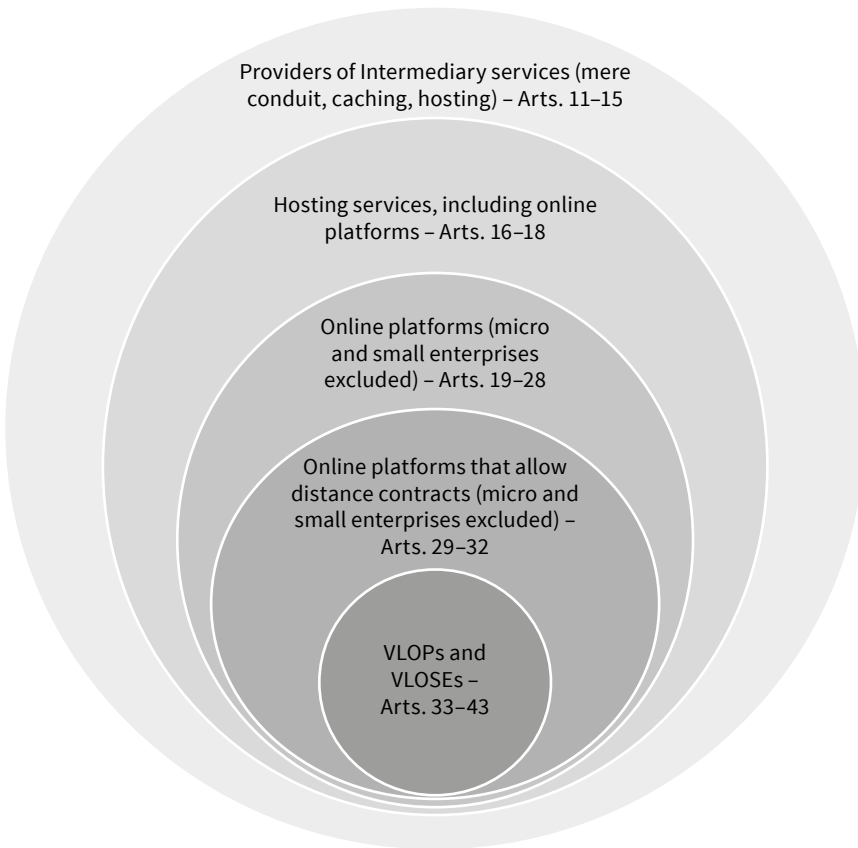


Figure 1. Layers of DSA Chapter III regulation framework¹⁴⁹

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 ítélezési 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 tükröz: 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 rögzös 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

VI. *QUI NON VETAT PECCARE, CUM POSSIT, IUBET* – THE CASE OF HUNGARY AND HOSTILITY ONLINE

ERIKA VÁRADI-CSEMA – LÁSZLÓ DORNFELD –
ROLAND LINDT

1. Introductory Thoughts

When discussing hate induced deviances, especially hate speech and bullying, the topic can possibly be approached as a conflict of certain fundamental values. More precisely, such actions are forms of expression that shall not, and usually do not, fall under the protection of the freedom of expression, since they violate other human rights like the right to human dignity, the right to privacy, the prohibition of discrimination, etc. without proper justification.

In Hungarian constitutional law theory, constitutionality is interpreted as an ensemble of principles including, among others, the fulfilment of certain ‘democratic principles’ like the provision of internationally recognised (minimum) standards of human rights and the need for specific institutions protecting the constitutional order from unconstitutional elements, such as constitutional courts and ombudsmen.¹ Nonetheless, in Hungary such issues, including hate speech, were not discussed in detail on a constitutional level for a longer period of time due to historical peculiarities – between 1949 and 1989, the socialist legal framework did not provide real institutional protection for human rights. Thus, we find it necessary to briefly summarise the development of the constitutional protection system from 1949 and the relevant constitutional provisions currently in power before analysing criminal law related aspects.

¹ Pap, 2013, pp. 14–15. Cf. Trócsányi, 2014, p. 68; Varga, 2015, pp. 10, 22–25, 41; Jakab, 2020, p. 76; Tóth, 2020, pp. 103, 114–115; Tóth, 2024, pp. 198–203.

1.1. The Constitution of the Hungarian People's Republic and Fundamental Rights (1949–2011)

After World War II, the fascist dictatorship was ended by the Soviet army and a provisional period commenced. A major development of this era was the transition from being a monarchy to a republic.² The act by which this constitutional change was enacted was accompanied by another one that encompassed a certain form of protection of fundamental rights by establishing sanction for those public officials who, while exercising their power, violated the rights of citizens without lawful reason.³ At the time, Hungary had no written constitution but several sources of law regulating constitutional questions, including pieces of legislation in the field of freedom of religion, freedom of assembly, freedom of association, etc. In other words, the law on human rights protection was fragmented and incomplete.

In 1949, after the fusion of the Hungarian Communist Party and the Social Democratic Party, the newly formed Hungarian Workers' Party seized power, thus creating a one-party political system, and the first written constitution of Hungary, the Constitution of the Hungarian People's Republic (hereinafter: Constitution)⁴ was adopted. The document contained mainly declarative measures, providing no real guarantees against state power.⁵ Furthermore, the rights encompassed were not considered 'human rights' or 'rights of citizens but 'rights of workers', and no special mechanism was established to provide remedy for violations of such fundamental norms. Although the National Assembly⁶ had the exclusive competence to adopt acts, the so-called Presidential Council of the Hungarian People's Republic (hereinafter: PCHPR), functioning as a collective head of state, exercised its powers whenever the National Assembly was not in session. Pieces of legislation adopted by the PCHPR were called 'decree-laws'.⁷

2 Art. 2(1) of Act I of 1946. On the significance of the act concerned in the history of Hungarian public law, see: Kukorelli, 2017.

3 Act X of 1946. Although, such a provision was not unprecedented in Hungarian legal history. Act V of 1878 (hereinafter: Code Csemegi), the first criminal code of Hungary, adopted during the era of the Austro-Hungarian Monarchy (1867–1918), already ordered to punish those public officials who, by abusing their power, violated one's right to liberty. See: Art. 193 of Code Csemegi. See also: Sári, 2004, pp. 26–27.

4 Act XX of 1949. This document was implementing the mentality of the 1936 Soviet Constitution, usually referred to as the Constitution of Stalin.

5 Cf. Sári, 2004, p. 24. Therefore, from the perspective of political sciences, it is considered a formal constitution. Horváth and Völgyesi, 2020, p. 492.

6 National Assembly is the official designation of the parliament of Hungary (the authors).

7 The decree-law occupied a rather prominent place in the hierarchy of sources of law, since it had the 'second place' after the acts of the National Assembly, i.e. with one exception, no other source of law could contradict a decree-law. For the hierarchy, see: Bihari, 1984, pp. 44–45; Ádám, 1990, pp. 51–52.

Decree-laws had to be introduced before the National Assembly during the session following their adoption.⁸ In practice, the National Assembly had two or three sessions per year, as prescribed by the Constitution that did not last longer than a few days. Consequently, the PCHPR exercised the powers of the supreme body of popular representation for most of the year, without having been elected directly by the citizens.⁹ From a practical perspective, it can be stated that the working mechanism of the PCHPR served the transformation of the political will of the party into legally binding regulation.

Several changes were made during the socialist era at a constitutional level. Here, we only strive to highlight the major steps of development regarding the protection of fundamental rights. Therefore, joining the approach of Pál Vastagh,¹⁰ we decided to summarise three significant legislative events.

In the first place, we must emphasise the role of the amendment of the Constitution in 1972, also referred to as the revision of the Constitution.¹¹ From the perspective of fundamental rights, an important shift of terminology took place. The term ‘rights of workers’ became obsolete in the light of social development, thus the revised text adopted the term ‘rights of citizens’.¹² According to Ottó Bihari, constitutional guarantees of certain economic, social and cultural rights were also strengthened i.e. the normative value of the provisions concerned increased.¹³ Furthermore, an essential declaration also appeared: ‘[t]he Hungarian People’s Republic respects human rights.’¹⁴ This statement was considered the recognition of international standards in the area. Finally, a new general guarantee was placed among the general provisions of the related chapter, declaring that rules on fundamental rights and duties of citizens had

8 Art. 20(4)–(5) of the Constitution. On the other hand, some competences of the National Assembly could not be exercised by the PCHPR. The Constitution explicitly determined that only the National Assembly had the right to adopt its amendment. Later, the extent of the power of substitution was narrowed several times. See: Bihari, 1983, pp. 71–73; Bihari, 1984, p. 233; Ádám, 1990, pp. 270–271.

9 Bihari, 1983, pp. 238–241; Horváth and Völgyesi, 2020, p. 495. Another special treat of the PCHPR worth mentioning that differentiates it from its major constitutional alternative, the president of the republic, was that its decisions did not require the countersignature of a minister, therefore it held real political responsibility, at least in theory. Initially, it also had the right to annul the unconstitutional law, decision or measure adopted by any state body with the exception of the National Assembly. See: Arts. 21(3) and 20(2) of the Constitution.

10 Vastagh, 2019, pp. 46–47.

11 Vastagh, 2019, p. 46.

12 See: Chapter VII. of Act I of 1972.

13 Bihari, 1983, pp. 76–78.

14 Art. 54(1) of Act I of 1972.

to be prescribed in the form of acts,¹⁵ i.e. a restriction on the legislative competence of the PCHPR was introduced. Although not closely related to the revision of 1972, it should be mentioned that two major human rights conventions, the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social and Cultural Rights were transposed in 1976.¹⁶ Despite the indisputable positive change in the wording of the Constitution, *sui generis* bodies of constitutional protection were still not created.

The second remarkable amendment took place in the first half of the 1980s. The major novelty was the introduction of the so-called ‘Constitutional Council’ (*Alkotmányjogi Tanács*).¹⁷ These days, the significance of this body is rather questionable. Existing as a commission of the National Assembly, its elected members were also members of the National Assembly. The Constitutional Council had to make reports for the National Assembly regarding its activity and its members could be recalled.¹⁸ This kind of dependence rendered real constitutional control impossible. Moreover, its competences were rather ineffective, since it did not have the right to repeal unconstitutional norms, but could only call on state bodies with legislative competences to take action. The right to suspend the exercise of problematic norms was also a relatively weak measure.¹⁹ András Holló, former judge of the Constitutional Court of Hungary describes the Constitutional Council as a political body, citing the respective statements of the minister of justice of the era and states that loyalty towards the Council of Ministers was one of its major characteristics.²⁰ The non-legal character of the Constitutional Council is well-proven by the fact that its first president, Rezső Bognár, was a professor of natural sciences with no prior legal experience.²¹ As Péter Sólyom argues, the establishment of such an institution was a step forward from the uncontrollability of the National Assembly, but a ‘timid’ one. Real legal reasoning was a ‘tolerated wrong’ that had to be restricted to the greatest extent possible.²² In summary, the Constitutional Council was a necessary

15 Art. 54(3) of Act I of 1972.

16 Decree-laws no. 8 and 9 of 1976.

17 According to the amended text, its purpose was to verify the constitutionality of laws and legal directives. In certain cases, it had the right to suspend the exercise of unconstitutional sources of law. In contrast, it was not granted the power to exercise this right against the unconstitutional acts of the National Assembly, the decree-laws of the PCHPR and certain decisions of the Supreme Court. See: Art. 1 of Act II of 1983.

18 Arts. 3, 6–7 of Act I of 1984.

19 Arts. 18–20 of Act I of 1984.

20 Holló, 1997, pp. 38–43.

21 Horváth, 2023, p. 94.

22 Sólyom, 2021, p. 5.

but practically insignificant step in the history of the Hungary constitutional protection system.²³

The third event in 1987 can be interpreted as a kind of preparation for the regime change. A short but significant amendment was adopted, according to which the competence of the PCHPR was further narrowed. More precisely, the power of substitution no longer contained the right to adopt decree-laws in certain legislative subject matters that belonged to the exclusive competence of the National Assembly.²⁴ Therefore, the political will of the party could not be implemented anymore through a simple legislative procedure. Hence, the private sphere gained an important protective guarantee against state power. The legislative subject matters in question were placed in the Act on Legislation²⁵ and were divided into three subcategories: (i) issues related to social order and its main institutions; (ii) issues related to economic order; and (iii) fundamental freedoms and duties of citizens. From our point of view, the latter is of primordial importance, including individual freedoms, which were not enumerated precisely in the act, and rules regarding the press.²⁶

After years of preparation, from a regulative point of view, regime change took place through Act XXXI of 1989, which was theoretically an amendment of the Constitution, but practically rewrote the vast majority of the provisions that were in force until then, thus creating a legal system based on democratic values.²⁷ As a consequence, the Constitutional Court of Hungary (hereinafter: CC) was established as a modified version of the Austrian model.²⁸ Subsequently, the main result of the first decade of CC was the interpretation of the content of fundamental rights. Here, we shall highlight a CC decision related to hate speech that examined the legality of certain criminal offences in light of the freedom of expression.²⁹ As the conclusion of the case, a provision was repealed from the criminal offence 'agitation against the community'.³⁰ Summarising the famous *obiter dictum* of the decision, László Sólyom³¹ stated that the CC, upon the issue of agitation against the community, connected rule of law with democratic

23 For more details on the working mechanism and statistics, see: Holló, 1997, pp. 46–60; Horváth, 2023, pp. 93–96.

24 Act X of 1987.

25 Arts. 2–5 of Act XI of 1987.

26 Arts. 5(b) and 5(d) of Act XI of 1987.

27 For further information, see: Gosztonyi, 2020.

28 See: Act XXXII of 1989.

29 Decision no. 30/1992. (V. 26.); for the detailed content and critics, see: Gárdos-Orosz, 2021.

30 Art. 269(2) of Act IV of 1978.

31 First president of the CC, later President of the Republic of Hungary. For a brief introduction on his legacy, see: Koi, 2023.

values; constitutional protection for incitement to hatred would be contrary to the political and value system expressed in the Constitution.³² The mentioned CC decision was followed by a number of cases challenging the legitimacy of criminal offences that constituted the restriction of the freedom of expression.³³

After the elections of 2010, the government commenced a process of codification, including the revision of the Constitution itself. As a result, the Fundamental Law of Hungary (25 April 2011) (hereinafter: Fundamental Law) was adopted and entered into force on 1 January 2012, thus repealing the Constitution.

1.2. The Constitutional Foundations of the Freedom of Expression Today: The Fundamental Law of Hungary

Article IX(1) of the Fundamental Law declares that '[e]veryone shall have the right to freedom of expression. Further norms of the provision guarantee the freedom and diversity of press and the rule of equal opportunity to spread ideas for political movements during the elections, in order to provide the 'formation of a democratic public opinion'.³⁴ When discussing hate speech, the aim is to define legitimate restriction of the discussed freedom, therefore the rule on possible restrictions shall be introduced.

According to Article I(3) of the Fundamental Law, '[the] rules for fundamental rights and obligations shall be laid down in an Act. A fundamental right may only be restricted to allow the effective use of another fundamental right or to protect a constitutional value, to the extent absolutely necessary, proportionate to the objective pursued and with full respect of the essential content of that fundamental right'. The cited general rule on possible restrictions is usually divided into two subsets of criteria: formal and material criteria. The obligation to lay down such rules in an Act, and no inferior source of law, is clearly a guarantee that only the state body with 'direct legitimacy', the National Assembly has the right to establish restrictions. The text encompasses the following material criteria:

- the restriction must have the aim to allow the effective use of another fundamental right or to protect constitutional value;³⁵
- the necessity-proportionality test; and

³² Sólyom, 2001, p. 94.

³³ In this subchapter, we do not intend to discuss the relevant decisions in detail. For a list on the cases, see: Szomora, 2024, p. 328.

³⁴ Arts. IX(2) and IX(3) of the Fundamental Law.

³⁵ Constitutional value has a broad and ever-changing approach. For a possible constitutional interpretation, see: Koi, 2005, 77–79.

- the restriction must fully respect the core content of the restricted right.³⁶

Furthermore, the Fundamental Law also contains specific rules on restriction of specific fundamental rights. This is the case of the freedom of expression too. Article IX(4) states that '[t]he right to freedom of expression may not be exercised with the aim of violating the human dignity of others'. With such a declaration, the Fundamental law creates a hierarchy in the relation of the freedom of expression and the right to human dignity, making the latter always superior. After the fourth amendment of the Fundamental Law, Article IX(5) introduced the concept of the protection of dignity of the 'Hungarian nation or of any national, ethnic, racial or religious community', a norm that provides the opportunity for the members of such communities to enforce their claims in court against expressions that constitute violation of the community's dignity of which they are part of. Methods provided will be discussed below, here we just refer to the fact that the dignity of communities has not yet been interpreted exhaustively by the CC, and its relation to human dignity is also unclear.^{37, 38}

Having summarised the brief history of Hungarian constitutional development after World War II and having discussed the constitutional foundations currently in force concerning the freedom of expression and its possible restrictions, the next subchapter will further elaborate its borders through the explanation of the most relevant criminal law and civil law regulation.

2. Regulation of Hate Speech

Hate speech is criminalised under Section 332 of Act C of 2012 on the Criminal Code of Hungary (hereinafter: Criminal Code), codified under the offences against public order, under the heading of 'incitement against the community'. However, before analysing the current legislation, it is essential to briefly describe the historical development of the Hungarian legislation, with particular reference to the earlier decisions of the CC, as this is where the political and

³⁶ For the detailed interpretation of these criteria, see: Paulovics, 2013; Gárdos-Orosz, 2018; Erdős, 2021.

³⁷ Although there were decisions related to the dignity of religious communities that strived to solve the doctrinal questions, these were criticised by scholars for not giving conclusive answers. For example, see: Kovács, 2021, pp. 352–355; Csink and Csink, 2024, pp. 11–12.

³⁸ For a deeper analysis on the protection of the freedom of expression, see: Koltay, 2021.

professional debates on hate speech culminated, and these decisions are still decisive in defining the regulatory framework of the issue.

2.1. History of Incitement Against the Community

In Hungary, hate speech legislation dates back to the Code Csemegi. Section 172 of Act V of 1878 already included the criminalisation of ‘inciting one class, nationality or religious denomination to hatred against another’, if this was done in the manner described in Section 171, ‘publicly, by word, [...] by distributing or exhibiting a print, document, or pictorial representation’. Section 8 of Article III of Act III of 1921 on the More Effective Protection of State and Social Order made it a misdemeanour to punish anyone who uses an expression or commits an act of defamation against the Hungarian State or the Hungarian nation. After World War II, socialist legislation, both in Act XLVIII of 1948 and in the Criminal Code of 1961, regulated agitation as a crime against the state, giving it a strong political connotation, as it was used to defend the party state. The 1978 Criminal Code retained agitation as an offence against the state (Section 148), but introduced a new offence called breach of the peace (Section 269). At the time of the regime, Act XXV of 1989 gave Section 269 a new title, agitation against the community, while removing the offence of agitation from the offences against the state in the Penal Code.³⁹

The basic constituent elements of the offence were as follows: anyone who incites hatred against the Hungarian nation or a nationality, or a people, religion or race, or a group of the population in public commits a criminal offence. In addition, there was a privileged offence (defamation), if the offender used an insulting or degrading term against these groups. The CC annulled the latter provision in the aforementioned Decision no. 30/1992. (V. 26.), since, according to point V of the explanatory memorandum, only the incitement contained in the basic provision of the offence meets the level of danger (*‘clear and present danger’*) which makes the restriction of freedom of expression necessary and proportionate. An abstract, potential threat to public order is not in itself a sufficient ground for restricting freedom of expression. Three interpretations of the decision have emerged in the legal literature: the first group has interpreted it as a mandatory application of the US-style *clear and present danger* standard; the second group argues that, even if it does not follow from the decision, a real danger must nevertheless follow from the expression of opinion; while the

39 III. sz. melléklet – A gyűlöletbeszéd büntetőjogi szabályozása és az Alkotmánybíróság gyakorlata [Online]. Available at: https://kuria-birosag.hu/sites/default/files/joggyak/iii._sz._melleklet_-_a_gyuloletbeszed_alkotmanyos_osszefuggesei.pdf

traditionalist criminal law advocates argue that the ability of the communication to incite hatred is in itself sufficient for the offence to be committed.⁴⁰

The next important decision of the CC was no. 12/1999. (V. 21.), which was based on the 1978 Penal Code, which included the offence of ‘committing other acts capable of inciting hatred’. Here, the CC referred to its earlier judgment and to the fact that the amendment lowers the threshold for restrictiveness.

In December 2003, the text was again amended, and the legislator again sought to create a privileged case by including in the text the criminalisation as a misdemeanour of ‘defaming or humiliating another person or persons on grounds of national, ethnic, racial or religious affiliation’. However, the President of the Republic did not sign it, but sent it to the CC for a preliminary review. The Minister of Justice, who proposed the amendment, gave a detailed justification, preferring a grammatical rather than a historical interpretation, and then referred to the country’s international legal obligations. The CC, however, in its Decision no. 18/2004. (V. 25.), found the bill unconstitutional, arguing that the legal protection criterion of the Constitution and the necessity-proportionality test of the CC must be taken into account when complying with international obligations.

More importantly, the decision took a clear step towards introducing the *clear and present danger* test into Hungarian law. According to the reasoning, ‘[a] restriction on the right to freedom of expression in the case of ‘incitement to hatred’ is imposed because of the infringement of the exercise of an individual fundamental right or the imminent danger thereof. Finally, it is important that the danger to public tranquillity is not merely hypothetical, and that at least a hypothetical feedback (the communication is capable of disturbing public tranquillity) is indispensable, since the intensity of the disturbance of public tranquillity ‘above a certain level (‘clear and present danger’) justifies a restriction of the right to freedom of expression.’ In the assessment of András Koltay, the CC ‘reversed’ the reasoning of its own 1992 decision and, standing on the basis of an inaccurate quotation, made the above-mentioned standard part of its practice.⁴¹

In February 2008, an attempt was made to reintroduce into the 1978 Penal Code the offence of ‘defamation’, which would have punished the use of a term or a rumour capable of defaming the honour of a member of a group, or of insulting his or her human dignity, or a gesture that recalled or referred to an authoritarian regime or an idea, or that was capable of defaming honour or insulting

⁴⁰ For more details of the debate and related literature, see: Koltay, 2013, pp. 92–97.

⁴¹ Koltay, 2013, pp. 107–109.

human dignity. The explanatory memorandum argued that, despite the very similarity of the offence, this is not a lesser form of incitement against the community. In this regard, it pointed out that the two offences had different legal subject matter: while incitement against the community was substituted for offences against public order, the proposed act of insult would have been a crime against liberty and human dignity. The President of the Republic again refused to sign the Act and sent it to the CC for a preliminary review, which ruled that it was unconstitutional in its Decision no. 95/2008 (VII. 3.). The judiciary argued that the law did not meet the requirement of clarity of the norms and did not make clear exactly what conduct could be held liable. Moreover, as an intangible offence of endangering, it is not necessary for a result to be established, i.e. the honour or dignity of a specific person need not be damaged. The CC reasoned that action against racist speech in general cannot be constitutionally justified.

2.2. Current Regulation of Hate Speech and Related Offences

The Criminal Code, in the case of the offence of incitement to hatred in Section 332, the most significant change compared to the previous legislation is the inclusion of disability, gender identity and sexual orientation among the protected groups. However, this is more a matter of principle, since it was already covered by the expression ‘certain groups of the population’, which is also present in the text in force.⁴² The explanatory memorandum states that the legislator changed the name of the offence from incitement to sedition specifically in order to be consistent with the content of the CC decisions. The offence is punishable in the presence of the ‘general public’, which is not precisely defined in the interpretative provisions of the Criminal Code, which only mentions, by way of example, publication in the press, media, reproduction or electronic communications network. This means that committing an offence in the online space (e.g. by means of a comment or blog post) always fulfils the criterion of high visibility.⁴³

Proceedings were initiated against national radical activist and blogger Tamás Polgár ‘Tomcat’ Polgár under the 1978 Penal Code in connection with a blog post by him, which was reported by human rights organisations. In it, the author made remarks against the Roma population in Hungary and then called on his readers to beat up Roma people in groups as they stood in the streets. The Court of First Instance ruled in 2013 that the latter part of the article was a clear invitation to the reader to commit an act of violence and that, given the author of the article,

⁴² Koltay, 2013, p. 120.

⁴³ For a deeper analysis of the criminal offence in question, see: Sántha, 2020; Mezőlaki, 2022; Nagy, 2023.

his readership and the comments accompanying the article, as well as the target group, there was a real risk that this would happen. The court, however, classified the rest of the blog post as falling within the scope of freedom of expression.

Following an overview of the legislation on incitement to hatred, we must also briefly consider the other elements of hate speech. Public denial of the crimes of the National Socialist or Communist regimes under Section 333, which is committed by denying, doubting, trivialising or seeking to justify the genocide or other acts against humanity committed by the two totalitarian regimes. This has been introduced in the Penal Code as part of the compliance with the EU Framework Decision 2008/913/JHA against racism. Originally, only denial of the Holocaust was criminalised, but later, with an amendment in May, denial of the crimes of the communist regimes was also included.⁴⁴ The CC ruled in Decision no. 16/2013 (VI. 20.) that the provision was not contrary to the Constitution, as it protected the dignity of the victims, social commitment and ultimately public peace.

The Criminal Code also raises interesting questions on the subject of the use of the authoritarian symbol under Section 335, which has also been the subject of long-standing controversy. It may be said that, according to the interpretation of the CC,⁴⁵ the use of symbols (images, symbols, wearing a garment) may also constitute political expression and are generally constitutionally protected. Symbols played an important role in totalitarian dictatorships and have continued to have political and social meaning since their fall. They may include:

- officially used symbols (e.g. the coat of arms or flag of a state or party); and
- symbols not directly linked to the regime (e.g. the Arpad's flag).

The criminal prohibition in these cases tends to cover only the first category, as in our country, where the depiction of the swastika, SS insignia, arrow cross, hammer and sickle, and the five-pointed red star are prohibited.⁴⁶

The CC ruled in Decision no. 14/2000. (V. 12.) that freedom of expression may be restricted if it is 'necessary in a democratic society'. However, the decision did not take into account the fact that the risk of a concrete harm necessary for the restriction of freedom of expression could not be established in the case at hand.⁴⁷ The European Court of Human Rights has over the years in several cases (in the case of the red star, in the Vajnai⁴⁸ and Fratanoló⁴⁹ cases; in the

⁴⁴ Smuk, 2019, pp. 241–242.

⁴⁵ CC Decisions no. 95/2008. (VII. 3.); no. 13/2000. (V. 12.) and no. 14/2000. (V. 12.).

⁴⁶ Smuk, 2019, pp. 232–235.

⁴⁷ Smuk, 2019, p. 243.

⁴⁸ ECHR, case no. 33629/06. Vajnai v. Hungary.

⁴⁹ ECHR, case no. 29.459/10. Fratanoló v. Hungary.

case of the flag with the Árpád-stripe in the Fáber-case⁵⁰) held that the freedom of expression is not subject to a specific threat of harm. The European Court of Human Rights has ruled over the years that Hungary has violated freedom of expression, since the use of the symbols concerned does not always imply identification with dictatorial regimes.⁵¹

On this basis, the CC annulled the provision on the prohibition of authoritarian symbols in its Decision no. 4/2013. (IV. 21.). Subsequently, the National Assembly created a new definition of the offence, which is much narrower, requiring that the use of an authoritarian symbol must be ‘in a manner likely to disturb public peace, in particular by violating the human dignity or the right to respect of the victims of authoritarian regimes’. Although this is a solution to the problem, the introduction of the *clear and present danger* test, taken over from the practice of incitement, in case law following the amendment could lead to a severe narrowing of the scope of criminal liability, which was not the intention of the legislator. The offence is a subsidiary offence, so that it cannot be committed unless a more serious offence (incitement) is established.⁵²

In 2017, the amendment was again on the agenda with the bill T/14441., this time because of the products with the red star.⁵³ The most famous of these is Heineken beer, on the basis of which the press christened the bill Lex Heineken. The proposal would have made it a criminal offence to sell goods or services bearing an authoritarian symbol, but the Government could have exempted the prohibition if there was sufficient evidence. Although even the European Commission did not object to the proposal after a lengthy examination, it was not discussed after the political will to adopt it had disappeared.

2.3. Future Perspectives – Definition of Aggression on Internet

In November 2024, bill T/9996.⁵⁴ was introduced, which has the aim of fighting online aggression. To this end, it envisages the adoption of a new Section 332/A of the Criminal Code, called Aggression on Internet. As the text follows, any person shall be punishable who uses or publishes to the general public, by means of an electronic communications network, any expression, representation or image or sound recording which is likely to cause violent acts, to a certain person or

50 ECHR, case no. 40.712/08. *Fáber v. Hungary*.

51 Tóth, 2013, p. 52.

52 Smuk, 2019, pp. 245–246.

53 *Törvényjavaslat T/14441*. [Online]. Available at: <https://www.parlament.hu/irom40/14441/14441.pdf>

54 *Törvényjavaslat T/9996*. [Online]. Available at: <https://www.parlament.hu/irom42/09996/09996.pdf>

persons, that results in death or perpetrated with particular cruelty, or expresses an intention or desire to commit a criminal offence. As one can observe, the *modus operandi* is clearly described, thus this offence can only be perpetrated in the digital sphere. The fact that this is a subsidiary offence, not explicitly, but mainly related to incitement against a community, should also be noted. The second part of the definition encompasses a ground for exemption, if someone commits such an act for the purpose of disseminating information, education, science or art, or about events in history or current affairs, provided that the act is not intended to cause fear. The new provision is likely to enter into force on 1 January 2025.

2.4. A Civil Law Tool Against Hate Speech

As part of the regulation on personality rights, Act V of 2013 on the Civil Code (hereinafter: Civil Code) establishes a practical opportunity for members of violated communities, as envisaged by Art. IX(5) of the Constitution, to enforce their rights in court.⁵⁵ This special form of enforcement has strict limits, e.g. the thirty-day term of preclusion, but also provides procedural solutions that ease the situation of the community members concerned regarding the taking of evidence.⁵⁶ It should also be emphasised that the Civil Code also provides the right to enforce personality rights for the public prosecutor if the violation additionally harms public interest.⁵⁷

3. Regulation of cyberbullying

The Criminal Code does not contain a specific, named offence of cyber intimidation. There are, however, a number of elements which can be applied, with varying degrees of consistency, to certain forms of cyber-fraud. These are (from most to least similar):

55 'Any member of the community may enforce his personality rights within a thirty-day term of preclusion from the occurrence of a legal injury that was committed with great publicity in relation to some essential trait of his personality, his belonging to the Hungarian nation or some national, ethnic, racial or religious community, and is grossly offensive to the community or unduly insulting in its manner of expression. With the exception of relinquishing the material gain obtained through the violation of rights, any member of the community may enforce any sanctions of the violation of personality rights'. Art. 2:54(5) of the Civil Code.

56 For more details, see: Barzó, 2018, p. 185; Pribula, 2023.

57 Art. 2:54(4) of the Civil Code.

- harassment (Section 222 of the Criminal Code);
- relationship violence (Section 212/A of the Criminal Code);
- humiliation of a vulnerable person (Section 225 of the Criminal Code);
- assisting suicide (Section 162 of the Criminal Code);
- defamation (Section 226 of the Criminal Code);
- making and publishing a false record or photograph capable of defaming
defamation (Sections 226/A to 226/B of the Criminal Code);
- insult (Section 227 of the Criminal Code);
- coercion (Section 195 of the Criminal Code);
- extortion (Section 367 of the Criminal Code).

Before discussing the individual offences in detail, it is worth pointing out that cyber intimidation does not have a uniformly accepted definition. In the following, the concept in the theoretical chapter will be the basis for the proper application of the definitions, i.e. the existence of the following conceptual elements will be examined:

- an assault of some kind intended to intimidate the victim;
- it takes place in the online space, using an electronic device;
- one-off or repeated behaviour;
- subordination.

3.1. Harassment

The most similar offence to cyberbullying in the Criminal Code is harassment. This similarity is also due to the fact that the phenomenon is often referred to in public discourse as online harassment, which is not correct, as the two concepts are not fully compatible. However, there is a common intersection where cyberbullying can be considered as online harassment.

Harassment is defined in the Criminal Code. Chapter XXI of the Criminal Code, under the offences against human dignity. The right to privacy has been previously derived by the CC from the general right to human dignity. Harassment has two elements, the first of which is harassment under Section 222(1) of the Criminal Code, where harassment is defined as conduct that is systematic or persistent or intentional, where the purpose of the offence is to intimidate the victim or to arbitrarily interfere with his or her privacy. This is a subsidiary offence and can only be established if no other more serious offence is committed.⁵⁸

⁵⁸ Monori, 2016, p. 248.

The other predicate offence also has a purpose, where the purpose is to instil fear, and the offence has two turns in terms of conduct:

- threatening another person or, in respect of that person, his or her relative, with the commission of a criminal offence of violence against a person or of an offence causing public danger; or
- creating the appearance that an event is about to occur which is injurious to or directly endangers the life, limb or health of another.

The essential difference between the two basic elements is that while the first covers a longer process, the second relates to a single act of threatening behaviour. The offence of harassment has been the subject of much scrutiny in Hungarian jurisprudence and is not without its critics⁵⁹ The section also contains four further qualifying cases where someone commits the offence:

- injuring his or her spouse, former spouse, common-law partner or former common-law partner,
- to the injury of a person under his or her education, care, custody or care or treatment,
- abusing his or her position of power or influence; or
- to the detriment of a public official, at a place or time incompatible with his or her official duties.

Where cyber intimidation is construed as harassment, the question of the factual nature of the offence should be examined. As harassment has not been defined by the legislator, it is for the legislator to give it the appropriate content. According to various commentaries, harassment is conduct which causes significant disruption or disturbance to the victim's private life and regular activities. According to a judgment of the Curia⁶⁰, harassment, which is one of the basic elements of harassment, is a one-sided, continuous conduct which can be achieved by words as well as by actions. In the case of cyberbullying, in order for the facts to be established in this case, the harassment must be carried out by means of a telecommunications device. A large proportion of harassment already involves the use of such means by perpetrators.

On the issue of regularity, Zsuzsanna Éva Monori stresses that it is important that the fact that the victim seeks contact attempts and that the same number of attempts are reciprocated by the accused precludes the existence of a *prima facie* case, as does the fact that the victim is unaware of the harassment.⁶¹ Since

⁵⁹ For example, see: Bérces, 2017, pp. 454–462.

⁶⁰ BH+ 2011.12.518.

⁶¹ Monori, 2016, p. 253.

cyberbullying often takes place in such circumstances (the victim seeks the company of the bullies for social reasons or behind their back, e.g. in an online forum), this may exclude the establishment of the offence of harassment.

In relation to the purpose, it can be noted that in the case of ‘intimidation’, the fear of the victim, as a result, does not actually need to develop in order to be established. In comparison, the concept of ‘arbitrary interference’ would be difficult to define. It is considered that it stops in cases where the victim expresses a clear rejection or objection at the time of contact, failing which the harasser may – also according to curia practice – defend himself by claiming that he did not know that the victim perceived these acts as harassment. The victim must be able to perceive the contact, but this is a purely formal criterion, and it is not necessary for him to know the content of the messages. The Internet space is characterised by greater reciprocity, anonymity and more effective ways of dealing with harassers.⁶²

Of the basic elements of harassment, harassment by harassment is the one that is most closely comparable to cyberbullying, as regularity is an essential element of the offence. Intimidation is presented as the purpose of the offence, which also corresponds to the concept. The question of subordination appears in the qualified cases, where the legislator has essentially assessed family ties and the position of power.⁶³

3.2. Relationship violence

The offence of relational violence was not yet included in the promulgation of the Act, but was inserted into the Act by Act LXXVIII of 2013 amending certain criminal acts, as Section 212/A of the Criminal Code, with effect from the entry into force of the Criminal Code. According to the Ministerial Explanatory Memorandum, ‘the character of the new, autonomous offence is further strengthened by the fact that, in addition to the more severe penalties associated with the new offence, the new offence, in view of the specific nature of the victims and the regularity of the offence, also criminalises new conduct not previously covered by the Criminal Code, in comparison with the existing offences; accordingly, the Act also criminalises violent conduct that does not rise to the level of assault but seriously offends the human dignity of the victim and economic incapacity.

The victim of the offence may be the parent of the offender’s child, as well as his or her relative, former spouse, former partner, guardian, trustee, guardian

⁶² Monori, 2016, p. 254.

⁶³ Parti, 2016, p. 122.

or ward living in the same household or in the same dwelling as the offender at the time of the offence or at any time in the past. The two basic elements of the offence have in common the element of habitualness and the conduct which seriously offends human dignity, humiliation and violence, depriving the victim of material property belonging to the common household or common property, thereby exposing the victim to severe deprivation.

In the first basic case, the basic offence of slight bodily injury or intentional defamation may be linked to the first basic offence; while in the more serious case, the basic offences of aggravated assault (committed with malice aforethought or purpose or to a person incapable of defence or of expressing his or her will, or to a person whose capacity to prevent the offence is limited by reason of his or her age or infirmity), grievous bodily injury, infringement of personal liberty or coercion may be linked to the first basic offence.

The offence is subsidiary and the first predicate offence is punishable only on the private initiative of the victim. Regularity is an important element of the offence, which means not only the number of occasions, the repetition, but also the existence of a consciousness linking these occasions. The Curia has also taken this position in a case-law decision, stating that for there to be regularity, there must also be a state of consciousness which, in addition to repetition, is linked.⁶⁴

The legislator's intention that the treatment of systematic violence as a criminal offence should not result in a reduction of the penalty can be seen from the legislative reasoning. Where the conduct necessary to establish the more serious cases is not regularly engaged in by the offender but is only occasional, it must be established as a separate, distinct offence.⁶⁵

When analysing the facts from the point of view of cyber intimidation, it can be said that both abuse of authority and subordination are implied, even if not explicitly included in the law. Systematicity is also an important element of the offence, as is cyber intimidation.⁶⁶

3.3. Humiliation of a vulnerable person

The offence of humiliation of a vulnerable person can be found in Section 225 of the Criminal Code and has been incorporated into Section 225 of the Criminal Code. According to the basic offence in paragraph (1), anyone who persuades another person to humiliate him/herself by taking advantage of his/her

⁶⁴ Criminal Principle Decision no. 17/2017, point I.

⁶⁵ László, 2020, pp. 68–69.

⁶⁶ Parti, 2016, p. 124.

vulnerable situation commits a misdemeanour. The offence is to induce the victim to behave in a humiliating manner. In the case of the victim, vulnerability is not specifically defined in the Act, but the Explanatory Memorandum makes it clear that it is to be interpreted in its ordinary sense, the Explanatory Memorandum giving as an example a homeless person in a seriously disadvantaged social situation.⁶⁷ The offence is subsidiary; the Explanatory Memorandum states that some of these acts were already punishable before, so that the offence was intended to criminalise only those cases which could not be punished under the existing criminal law.

The qualifying circumstances are defined in paragraph (2) as where the offender:

- gives or promises consideration in the course of inducing the offender to commit the predicate offence;
- records or makes available to the general public a recording of the person humiliating him or herself.
- The public at large, as mentioned above, includes offences committed on the internet, which makes this relevant to our topic.

What is new compared to the 1978 Penal Code is that the offence is punishable more severely under paragraph 3 if it is committed on a commercial basis. According to the Criminal Code and judicial practice, the offence is considered to be committed on a commercial basis if it is committed on a regular basis for financial gain. The emphasis is not on the degree of benefit derived, but on the fact that it is done on a regular basis.⁶⁸ The legislator may have been trying to respond to cases where someone regularly produces such content for a video sharing platform (e.g. Youtube), for the purpose of, say, viewing – and the resulting revenue.

The reason for creating the facts was that in recent years it has become increasingly common for people to upload videos on the internet where they persuade people in bad situations to commit degrading acts, e.g. paying homeless people to fight each other. Although the consent of the victim essentially excludes criminal liability, in these cases the vulnerability and subordination of the victims make it much easier to bend their will. It is not a precondition for the predicate offence that the act must be committed in front of another.⁶⁹

Many elements of cyber intimidation are present here, such as subordination, the perpetrator in a position of power taking advantage of his position,

⁶⁷ On the interpretation of ‘vulnerability’, see also: Huszár, 2022, pp. 308–309.

⁶⁸ BH 2015.8.212.

⁶⁹ Tóth, 2017, pp. 120–121.

and humiliation.⁷⁰ However, regularity is not a necessary element, but it is an important part of the concept of cyber intimidation. While the predicate offence and the qualifying offence can hardly be established in many cases of cyberbullying, the more serious qualification of commerciality is almost non-existent. The applicability of the facts is reduced by the fact that it is a subsidiary offence.

3.4. *Assisting a suicide*

It is important to note that the current Penal Code does not criminalise suicide or attempted suicide per se, but only assisting suicide. This offence has a long history in the history of Hungarian criminal law, as it was already included in the Code Csemegi. Unfortunately, the new challenges of the digital space have once again given it a sad topicality.

Assisting in suicide under Section 162(1) is a *sui generis* offence, the basic elements of which include inducement or aiding and abetting, and the perpetrator and passive subject can be anyone. The Act gives special protection to persons under the age of eighteen, and paragraph 2 of the Act therefore imposes a more severe penalty on an offender over the age of eighteen who persuades a person under the age of eighteen to commit suicide or who assists a person under the age of eighteen to commit suicide. In this case, coercion means an act of persuasion which results in the development of suicidal intent.

If the victim is under the age of 14 and dies by suicide as a result of the victim's persuasive behaviour, it is already punishable. Section 160 of the Criminal Code and carries a much more severe penalty. If the perpetrator's conduct only involves assistance, or if the victim under the age of 14 only succeeds in attempting to commit suicide but does not die as a result of the instigating conduct, then assisted suicide may be established.

The victim's mental capacity is relevant if he is incapable of expressing it. A criminal case law decision of the Curia⁷¹ declares that a person who is incapable of expressing his or her will is also incapable of deciding his or her will, i.e. the act can only be committed by coercion. The main cases are: childhood, pathological mental state, and coercion or threat.

In the context of cyber intimidation, the facts may be applied in certain cases. In this country, there are several known cases where someone has attempted suicide as a result of ongoing intimidation. This situation may be

⁷⁰ Parti, 2016, p. 123.

⁷¹ Curia criminal law decision 3/2013.

relevant if, during the intimidation preceding the suicide, the victim was constantly encouraged by his abusers to take his own life. Such a case is not yet well known in this country, but there are plenty of examples in the United States. However, from a dogmatic point of view, the correspondence between cyberbullying and the Criminal Code is rather weak. On the one hand, the offence does not in any way value subordination, regularity, nor is intimidation the aim of the act, but rather the result of it.⁷²

3.5. Defamation and Insult

Defamation and insult also have a rather long regulatory history, modern Hungarian criminal law has punished them since the Code Csemegi, but also has certain medieval and modern historical antecedents. The Penal Code of 1961 and the 1978 Penal Code regulated the offences in a manner similar to that of today. However, the offence of ‘insulting an authority or official’, which existed alongside these as a separate offence, was found unconstitutional⁷³ by the CC in 1994 and repealed.⁷⁴

Section 226 of the current Penal Code contains the offence of defamation, while Section 227 contains the offence of libel. The offence of defamation is committed by a person who asserts or publishes a fact or uses an expression directly referring to such a fact which is capable of defaming another person. A qualified case is committed where the defamation is:

- with a malicious motive or purpose;
- in a public place; or
- by causing substantial damage to his or her interests.

Insult is committed by a person who, in addition to the cases of defamation described above, in relation to another person

- (a) in connection with the performance of the victim’s duties in the exercise of his employment, public office or activities in the public interest; or
- (b) in front of a large audience

harms reputation. The same penalties shall be imposed on any person who commits insult by an act of violence.

⁷² Parti, 2016, p. 121.

⁷³ CC Decision no. 36/1994. (VI. 24.).

⁷⁴ For more on this see Tóth, 2017, pp. 97–107.

The legal subject matter of both offences is human honour, which, according to judicial practice, means, on the one hand, the social esteem, or reputation, of the victim and, on the other, his human dignity.⁷⁵ The practical distinction between the two is rather difficult to draw, as Zoltán Tóth points out. While damage to reputation typically affects self-esteem, the reverse is not always true.⁷⁶

The conduct of defamation is the statement, rumour (passing on information from another) or direct reference to a fact capable of damaging reputation. This is to be understood as emphasising a point from which the whole event can be logically inferred. The fact may be false or true, in the latter case the offence may be established if proof of the truth is not admissible or fails. The state of consciousness of the offender (whether he was aware of the falsity of the fact, good or bad faith) has no influence on the factuality of the offence. Establishment of the fact may be oral, written, visual (even an internet meme) or other.⁷⁷

The possible passive subjects and perpetrators of defamation, as well as the grounds for exclusion, are the same as for defamation. The conduct of the offender may be the same as that of defamation, provided that the statement of a fact liable to defame is not made in private and is not known to a third party. It differs, however, if there is no statement of fact but simply the use of a defamatory term. As we have already pointed out, the Internet offence always involves a high degree of publicity, which is present in some form in both offences.

Proof of the truth of the alleged fact (Section 229 of the Criminal Code) is a ground for exclusion from criminal liability, but according to judicial practice this does not extend to the mere expression of opinion, criticism, value judgement or defamation.⁷⁸ Proof of the truth is only required if it is justified by the public interest or the legitimate interest of any person.

The doctrinal correspondence between the facts under consideration and cyber intimidation is rather weak. Subordination and regularity are not at all an element of the facts. Nor does intimidation appear as an objective, but as a result. However, in practice, it may be applicable in many cases of cyber intimidation, provided that the level of intimidation does not reach the level necessary to establish harassment.

⁷⁵ BH2000. 285.

⁷⁶ Tóth, 2017, p. 110.

⁷⁷ Tóth, 2017, p. 111.

⁷⁸ BH2007.365.

3.6. *False audio or video recording*

Act CLXXVIII of 2013 introduced the offences of ‘making a false sound or image recording capable of defaming’ (Section 226/A) and ‘making public a false sound or image recording capable of defaming’ (Section 226/B), which have been in force since November 2013. The first offence, making a recording, is a subsidiary offence, in fact it is a *sui generis* preparatory offence of disclosure, and can only be established if the recording is not disclosed.

Accordingly, the wording of the two offences is largely the same: making a recording is established when a person makes a false, falsified or untrue sound or image recording with the intention of defaming another or others, while disclosure is established when the offender makes the recording available.

Both offences have as their object the defamation of others and can therefore only be committed with a direct intent, the perpetrator’s consciousness must be aware that the recording is untrue or false. In the case of the offence of ‘making public’, it is a qualified offence if it is committed in public or with substantial damage to the public interest. The offence of ‘making available’ does not require that the recording be made available to anyone, it is sufficient that it has been published (e.g. uploaded to a social networking site or file-sharing site).⁷⁹

Looking at the correspondence with cyber intimidation, it can be said that the doctrinal link is rather weak. It does not involve either a position of power, subordination or regularity.⁸⁰ In practice, it may be relevant in cases where malicious images or memes of someone are created or published for the purpose of intimidation.⁸¹

3.7. *Other Offences*

Two other offences worth briefly mentioning in relation to cyberbullying are coercion (Section 195 of the Criminal Code) and extortion (Section 367 of the Criminal Code).

The offence of coercion is committed when the offender, by force or threat, forces the victim to do, not to do or to tolerate something, thereby causing substantial damage to the victim’s interests. The offence is coercion of the victim, which means that the victim does not act of his or her own free will but acts under external coercion. In the case of violence, it is important to emphasise that it can only be violence against a person, but any form of threat can be a factual matter.

⁷⁹ Tóth, 2017, p. 122.

⁸⁰ Parti, 2016, p. 120.

⁸¹ On the topic of internet memes, see: Kiss, 2016, pp. 350–360.

The offence has two outcomes: first, that the victim does, does not do or tolerates something against his or her will, and second, that this involves a significant loss of interest, which does not necessarily have to be suffered by him or her.

The dogmatic equivalence of coercion with cyber intimidation is rather low. Neither subordination nor regularity is an element of the offence, and intimidation is only a result, not an aim.⁸² It may be relevant in the context of cyber intimidation if, for example, the abusers use threats to prevent the victim from seeking help and thus put an end to the intimidation.

Extortion occurs when someone, for unlawful gain, coerces someone else to do, not do or tolerate something by force or threat, causing financial loss. The offence consists of two elements: first, coercion by threat or force, and second, passive action, inaction or acquiescence. In the previous criminal legislation, the term ‘causing damage’ was used, whereas the result is now ‘causing pecuniary damage’, which is a much broader concept, since it also includes loss of pecuniary advantage. Since the offence is intentional, it can only be committed with a direct intent.

Compared to cyber intimidation, there is also very weak doctrinal similarity. As with coercion, subordination and systematicity do not occur as an element of the offence, and intimidation is merely a result.⁸³

4. Focus on Prevention and Particularly Vulnerable Groups

In Hungary, as in other countries, this issue is a priority. Nonetheless, there is currently no specific criminal offence in the Criminal Code which fully covers the conceptual elements of cyberbullying. However, with the spread of information and communication technologies and the arrival of new generations socialized in the world of Internet, the number of problems and abuses has increased, as has the sensitivity of citizens to these issues.

For a long time, however, professional attention has focused ‘only’ on harassment – whether at school or at work. In this regard, the first such research specifically on bullying was carried out by Erika Figula in the early 2000s⁸⁴ and the first research specifically on cyberbullying was coordinated by György Virág almost 10 years later.⁸⁵ The history of domestic research, which was elaborated

⁸² Parti, 2016, p. 119.

⁸³ Parti, 2016, p. 120.

⁸⁴ Figula, 2004.

⁸⁵ Virág et al., 2014.

in detail by Gabriella Kulcsár,⁸⁶ shows how far the profession has come in the last few years.

Criminal law is the ‘sanctioning keystone’ of possible state and legal responses. It can only be used as an *ultima ratio*. Accordingly, the state seeks to use other instruments, and the focus is on prevention, on non-judicial means of dealing with the problem, and not primarily on the criminal sanctioning of such behaviour. There are also a number of programs and good practices aimed at detecting risk behaviour and warning signs as early as possible and dealing with them quickly, locally and effectively.

Domestic activities are diverse and can be grouped according to many criteria. There are:

- programs funded by the public sector (e.g. the Internet Hotline of the National Media and Infocommunications Authority) and other organisations (e.g. the Hintalovon Foundation’s Nemecsek program);
- programs aimed at general crime prevention (e.g. Blue Line Helpline, telephone number 116 111 [free of charge, 24 hours a day]) or specific thematic programs (e.g. Internet Safety Hotline);
- anti-bullying programs (e.g. Round Table for School Safety) and programs specifically aimed at preventing online bullying (e.g. ‘Online against online bullying’ [Education Office’s teacher training courses]);
- programs focusing on perpetrators (e.g. ENABLE program), victims (e.g. Internet Hotline) or other actors (e.g. educational institutions, especially ‘NyugiOvi Program’);
- programs related to the detection, prevention and management of bullying (e.g. School Watchdog Program) or its consequences (e.g. Contemporary ‘NETMENTOR’ Program);
- etc.

In general, however, it is important to underline that a significant number of these programs and solutions are specifically targeted at minors and children. This is partly linked to the fact that this age group is particularly vulnerable to information and communication technologies; and partly to the fact that the protection of the interests of certain particularly vulnerable groups (e.g. women) is a priority at both EU and national level.

The programs are characterized by methodological diversity, in terms of the level of intervention, depth, nature and duration of the programs. The

⁸⁶ Kulcsár, 2024, pp. 29–40.

applied methods can also be very diverse. However, research⁸⁷ has confirmed that longer-term results have been achieved by solutions that focus on restoring relations between the parties involved and on reparation to the victims.

4.1. From the Digital Strategy for Child Protection to the National Crime Prevention Strategy

At the strategic level, two important sources should be mentioned separately: the *Digital Strategy for the Protection of Children*, which, although narrowed down (target group and legal area), specifically addresses the phenomenon under investigation, and the *National Crime Prevention Strategy*, which aims to address the phenomenon as one of the priority problems from the crime prevention perspective, in connection with school bullying and school violence.

On the state side, the Digital Strategy for the Protection of Children (hereinafter: the Strategy), which was created in conjunction with a government decision⁸⁸ in 2016, should be highlighted. Point 8 of the latter also committed the Government to launch comprehensive and free training and education programs to prevent and address online bullying and harassment, and to improve media literacy among children, parents, teachers and other professionals working with children. Tamás Pongó underlines that this Government Decision is a landmark in many respects: in its terminology it has distinguished between online bullying and bullying (using the domestic scientific term for *bullying*) and in its training it has focused on a whole community approach, as children, parents, teachers and professionals should be involved in the training. This decision was the first visible political commitment to professional and inclusive action against bullying and cyberbullying.⁸⁹

The Strategy goes into detail on the concept of cyberbullying, which it describes as ‘one of the biggest threats in the online space’ and ‘more effective and efficient than physical violence in intimidating victims’. Referring to data from the EU, Kids Online project, Strategy shows that Hungarian children start to use the internet on their own at the age of 9 on average, with 60% of 9–16 years old using the internet regularly and a further 35% using the internet several times a week. Two thirds of the age group have their own profile on a social networking site. Among the various threats, 70% of respondents said they had been a victim of cyberbullying in the online space.⁹⁰

⁸⁷ Domokos, 2022.

⁸⁸ 1488/2016. (IX. 2.) Government Decision.

⁸⁹ Pongó, 2019, p. 164.

⁹⁰ The Strategy, p. 26.

In order to address the problems that arise, the Strategy does not in principle use punitive sanctions, but favours education, awareness-raising and prevention, with solutions such as mediation in schools or other alternative dispute resolution techniques.⁹¹ The toolbox only includes criminal law as a last resort. Cyberbullying is mostly a preparatory or instrumental act for more serious offences, of which usually only the intentionality of the less serious ones can be proven. According to the Strategy, the punishment of young people through detention does not have a preventive effect and may even be a factor contributing to adult criminality. Moreover, a punitive approach could lead to the mass criminalization of young people. In this context, Pongó considers that the current level of criminal legislation is satisfactory.⁹²

The National Crime Prevention Strategy addresses the issue of cyberbullying at several levels and in several forms.

The National Crime Prevention Strategy 2013-2023⁹³ focuses primarily on the school environment in several aspects. Educational establishments are a venue for the dissemination of crime prevention information and thus a channel for meaningful prevention activities. The staff of educational establishments play a key role in crime prevention. Kindergarten teachers, teachers, child protection officers, school doctors, nurses, social workers and school psychologists are involved in prevention not only as members of the child protection signaling system, but also as mediators of education, health promotion and health preservation, and crime prevention information.

This is particularly important if we consider that education is itself a fundamental activity of crime prevention, as it is through education that information, attitudes and behaviours related to safety and its preservation can be most effectively acquired by children and young people. Many crime prevention activities (e.g. teaching methods in lectures, training courses, camps, programs) should be based on education, thus reinforcing the impact of education.

At the same time, the school itself is also the scene of many crimes, be it bullying or violence in schools. It is important to note that, typically, in almost one fifth of the cases of violent public nuisance activities and violent crimes against the person, the places of perpetration were educational establishments, including dormitories and halls of residence; interestingly, the role of primary schools was particularly prominent.

⁹¹ Pongó, 2019, p. 165.

⁹² The Strategy, p. 104.

⁹³ 1744/2013. (X. 17.) Government Decision.

The National Crime Prevention Strategy 2024-2034⁹⁴ currently in force retains the previous approach in many respects but focuses on the specific links of cyberbullying to child sexual exploitation and child pornography, partly in light of the increased incidence of such crimes.

One of the priority activities that stands out among modern crime prevention activities is education, so running programs and organizing campaigns to prevent victimization in the online space is also a priority of the document.

The internet and social media provide an excellent opportunity for offenders to commit new types of crimes in the online space, while giving them the possibility of anonymity. Crimes committed in the online space are a threat to everyone. Prevention is even more important in case of online crime, which is why it is necessary to support campaigns and programs that help to develop self-defence mechanisms based on caution. The objectives of the campaigns include the tasks set out in Directive 2011/93/EU of the European Parliament and of the Council on combating child sexual abuse, sexual exploitation and child pornography.

On the other hand, the document in question also recognizes the importance of bullying in schools by identifying it as a priority risk factor and ‘alarm signal’ for offenders, which should be addressed as soon as possible, using appropriate prevention and education tools.

4.2. Professional Events, Organisational Initiatives

Several initiatives, both scientific and professional, have been taken place in Hungary, as part of both national and international cooperation, which indicates the importance and mobilising power of the issue. In addition to scientific research, they are also significant because they help to create the theoretical basis for concrete programs, to select appropriate methods and to develop methodologies.

4.2.1. Hungarian National Cyberbullying Conference

On 16 October 2016, the first interdisciplinary conference focusing specifically on cyberbullying in Hungary was held at the University of Szeged, Hungary, under the name of the Hungarian National Cyberbullying Conference (MOCK). The conference brought together representatives from academia, governmental and non-governmental organisations, and this diversity was reflected in the

94 1291/2023. (VII. 19.) Government Decision.

presentations. Among the speakers were Károly Huber, Chair of the Board of Trustees of the Foundation for a Responsible Society, Edina Kastory, Commissioner for Media and Communications, András Koltay, (then) member of the Media Council, and Katalin Parti, a researcher on the TABBY project.⁹⁵

4.2.2. Roundtable for School Safety

Another formal framework for professional cooperation, support and knowledge sharing is the ‘Roundtable for School Safety’, which has been operating since 2021. The declared aim of the KERIB⁹⁶ is to ‘bring together and invite for joint reflection and action professionals of programs and methods that offer solutions in this field and other organisations related to the world of public education’. Accordingly, theoreticians and practitioners, researchers and civil society, public and non-profit organisations, teachers’ unions and parents’ associations work together to prevent and address institutional violence and abuse in education/learning institutions and to help create a peaceful climate. To this end, they develop and promote methods for dealing with bullying and conflict management techniques.

In this context, it is important to point out that there are many conflict management services that can help to resolve the emotional consequences of bullying in schools. For example, school social workers employed by family support services in local partnerships are responsible for visiting the parties concerned, at the request of the school, and helping to deal with the situation, even involving the whole class. Thus, they can organise either mediation or another model (usually a community conference) to this end. And some schools already employ professionals who can use mediation techniques as teachers, with this as a priority. In cases where cyberbullying reaches the level of a criminal offence, mediation can be a supportive tool to help resolve and deal with the psychological consequences of bullying.⁹⁷

4.3. General and Specific Programs to Combat (Cyber)bullying

In order to prevent and tackle cyberbullying at home, a number of initiatives and specific programs have been launched, partly by the state and partly by NGOs.

Before presenting some of these programs in more detail, it is important to note that Gabriella Kulcsár, in the appendix to her monography published in

⁹⁵ Pongó, 2018, pp. 161–163.

⁹⁶ *Kerib* [Online]. Available at: <https://kerib.hu/>

⁹⁷ For more details, see: Csemáné Váradi, 2023.

2024,⁹⁸ has collected a bundle of proposals and programs that are professionally recommended, as follows:

- suggestions for educators/school professionals to deal with bullying and cyberbullying situations;
- suggestions for students in the event of bullying/cyberbullying detection or involvement;
- suggestions for parents in the event of their child being bullied or cyber-bullied (what to avoid and what to do).

4.3.1. *'NyugiOvi' (Relax Kindergarten) Program*

In addition to the numerous domestic programs, methodological adaptations and other solutions, it is worth mentioning the 'NyugiOvi Program',⁹⁹ which was developed entirely in Hungary. Its aim is to prevent future bullying in schools by intervening as early as possible. The sessions are mainly attended by pre-school and small school children. The program also includes teacher training and contact with parents.

4.3.2. *Peaceful Schools Program*

Among the general anti-bullying and awareness-raising activities, the 'Peaceful Schools Program'¹⁰⁰ is also worth mentioning, the main objective of which is to prevent and tackle institutional violence and bullying in educational institutions, taking into account the best interests of children, and to create a peaceful atmosphere. The program, originally American, was developed by Stuart W. Twemlow, psychiatrist and Frank C. Sacco, psychologist and expert on children's rights, and was adapted for Hungary by Csaba Horgász, psychologist, in 2006.

The specificity of the program is the target group it aims to mobilize. According to the program, all abuse requires an abuser, a victim and a bystander audience, but it is the attitude of the bystanders that determines what the initial situation turns into. They are the ones who, by their active, affirming action or by their indifference or passivity, can reinforce or encourage the negative impulses of the abuser; but they can also be the ones who can prevent the situation from escalating – if they are willing to intervene, to protect the victim or simply to express how much the abuser's behaviour is to be rejected and despised.

⁹⁸ Kulcsár, 2024, pp. 207–218.

⁹⁹ TKKI, 2017.

¹⁰⁰ See: Kissné Viszket and Horgász, 2013.

The specificity of the method is that it is institution-wide. In other words, the activity involves not only specific individuals, such as those potentially at risk, but also the whole wider school community, including parents, other staff (beyond teachers), and, where necessary, external professionals and volunteers. This enables the program to trigger change at systemic level. However, this internal motivation and commitment is an important condition for this. Without this, the goal cannot be achieved, and change will not be sustainable. Thus, the key words of the program are volunteering and creative use of internal resources. This will not only lead to a change of mindset in the daily functioning of the school community, but also to a change in the school climate.

4.3.3. *TABBY Project*

TABBY on the Internet (Threat Assessment of Bullying Behaviour in Youth Online) was an EU-funded project in five Member States between 2011 and 2013. Its theme was to assess the volume of bullying among children online and to address it in a complex way, with the aim of creating a risk assessment questionnaire that children can fill on their own, so that they can assess the seriousness of a given incident of online bullying and the possibilities for escaping it.¹⁰¹

The risk analysis questionnaire research carried out in the framework of the TABBY project concluded that the domestic student population is also significantly affected by this phenomenon, which is why it is important to address it. The project has sought to fill the knowledge gap in the country, producing free videos, a handbook and a peer mentor training program. A total of 600 people took part in the survey, divided into three groups according to their risk level. An important finding was that there is a strong link between bullying and cyberbullying. It turned out that the roles of victim and perpetrator are not the same in the two spaces, with a victim in the offline space easily becoming a perpetrator online.¹⁰²

The significance of the TABBY project is that it is to date the only major international cyberbullying project that have taken place in this country and has laid down the foundations for domestic research on the topic.¹⁰³

4.3.4. *Anti-Bullying Program*

In 2013, the Foundation for a Responsible Society was the first to launch Hungary's only organised anti-bullying program, the pilot of which ended on 31 March

¹⁰¹ Parti, 2012, pp. 224–226.

¹⁰² Pongó, 2018. p. 158.

¹⁰³ Pongó, 2018, p. 159.

2015. Although the intended focus of the program was on all forms of bullying, the pilot program focused only on bullying in schools and cyberbullying.

The two main pillars of the program are institutionalised solutions (program roll-out, studies, statistics) and case management. Students were also involved in prevention activities as ‘student ambassadors against bullying’, representing the objectives of the program at events and providing support in the peer community. Case management included legal advice and fact-finding, in the spirit that when bullying is present, prevention alone is not enough. The program also had its own training system.¹⁰⁴ Unfortunately, in the absence of adequate financial support, the program was not continued after the pilot ended.

4.3.5. ‘KiVa’ and ‘Online Against Online Bullying’

Developed in Finland and used in 90% of schools there, the program aims to prevent bullying and to deal effectively with cases of bullying. The second unit of the program, which can be divided into three units by age group (10–13 years old), was purchased by the Institute for Educational Research and Development in 2016 and three trainers were trained as part of a pilot project, which started with a pilot in three national educational institutions.

The adaptation study of the program is available in Hungarian.¹⁰⁵ According to the adaptation study, the intervention can be delivered using one of two approaches: (i) confrontational or (ii) non-blaming. In the first case, the abuser is confronted with the inappropriateness of his or her actions and is asked to stop the behaviour. In the second, he is not blamed for his actions but is asked to help the victim feel better. The latter approach is mainly used with younger children, while the former may be more appropriate with older children. An important element of an effective intervention is a proper procedure, where everything is thoroughly documented and a follow-up meeting is scheduled after the first meeting, and only at this second meeting is a possible sanction envisaged.¹⁰⁶

4.3.6. Online Against Online Bullying

The already mentioned *Online against Online Bullying program* will provide a wide range of training and educational materials for teachers from 2021 onwards.¹⁰⁷

¹⁰⁴ Pongó, 2018, pp. 159–160.

¹⁰⁵ Jármí, Péter-Szarka and Fehérpataky, 2015.

¹⁰⁶ Pongó, 2018, p. 164.

¹⁰⁷ *Pedagógus-továbbképzés publikus adatai* [Online]. Available at: https://www.oktatas.hu/pir/!PIR_PUBLIC/publikus-felulet/7970

The main aim of the contact hour training course is to prevent online bullying, including teachers as potential victims. Therefore, the program also addresses the need and principles for the development of school policies to protect teachers. The many topics covered include online bullying as a source of danger on the Internet, its forms and incidence, methodologies for combating it, the design of prevention activities and the protection of teachers in the online space.

4.3.7. *The ENABLE Anti-bullying Program*

Also piloted in 2018, significant was the introduction of the *ENABLE anti-bullying program*, which, subject to central funding, is available to interested institutions through the Pedagogical Education Centres. The ‘European Network Against Bullying in Learning and Leisure Environments’ is also noteworthy because it does not focus on a narrow area.¹⁰⁸ It approaches children as individuals in a complex interaction with the phenomenon; this holistic approach enables participating students to learn to exercise their fundamental rights, whether they experience bullying at home, at school or in other peer communities. The training, which is free of charge, is mainly aimed at older students of elementary, and students of secondary school. It is important to underline that they not only help to prevent and deal with bullying, but also, for example, to develop social-emotional skills and attitudes.

4.3.8. *Peer NETMENTOR Program*

Although it does not provide direct professional support, the *Peer NETMENTOR Program*, which has been operating since 2018 as part of the state Digital Well-being Program, provides significant referral support by training ninth-grade students in several secondary schools in Budapest and in rural areas to deliver Internet awareness sessions in their own schools or other institutions, and mentor their peers and younger students. This training includes a model cyberbullying session.¹⁰⁹

4.4. *Campaigns, Other Initiatives, Immediate Help Solutions*

Several *campaigns* have been organised in Hungary with the involvement of various professional and other organisations to raise awareness, share knowledge, warn of the dangers and sensitise people. For example, the Cartoon Network

¹⁰⁸ Jármi, 2019.

¹⁰⁹ Televele Médiapedagógiai Műhely Egyesület, 2018; for more details, see: *Kortárs NETMENTOR Program* [Online]. Available at: <https://digitálisgyermekvedelem.hu/netmentor>

has partnered with the Blue Line Foundation for Child Crisis and the National Professional Association of Head Teachers to organise a periodic campaign.¹¹⁰

The Foundation was a partner of the UNICEF Hungary *#nemvagyegyedül* (*you are not alone*) campaign¹¹¹ launched in June 2020 with the support of the ‘Generali a Biztonságért Alapítvány’ (*Generali for Safety Foundation*), involving famous Hungarian media personalities, stars, ‘celebrities’, who answered the questions received in an online talk show on Youtube, continuously posting about the dangers of cyberbullying, the help available (phone, email) and sharing their own negative experiences.

The seriousness of these activities is shown by the launch of a new campaign in September of the same year. The ‘*No to Cyberbullying*’¹¹² campaign was professionally supported by the Hintalovon Foundation and coordinated by the Central Media Group. This sensitisation program, involving public figures, aims to raise awareness of the existence of help and the importance of opening up about the psychological trauma caused, which, according to experts, is the first step towards recovery. Victims are not alone.

In July 2021, another campaign was launched, this time on TikTok, a favourite of children, under the hashtag *#offendingvoices*. The UNICEF campaign ‘Together Against Abusive Voices’¹¹³ was a great success, helped by the creative visuals, the techniques used, the video content and the involvement of well-known TikTokers.

However, sustained campaigns targeting all sections of society can only be effective if there are low-threshold services to which people can turn, even anonymously. Thus, the role of various general or specific helplines, online or telephone contact points is important.

Among the public initiatives, the *Internet Hotline of the National Media and Communications Authority* (hereinafter: NMHH), a legal helpline specifically for reporting online crime, is worth mentioning. Launched in 2005, the hotline has been operated by the NMHH since 2011 and its main objective is to ensure that illegal content on the Internet, mainly child pornography but also other criminal offences, can be removed quickly. In the fight against illegal online content, they work closely and effectively with the National Police Headquarters and the Cybercrime Department of the National Bureau of Investigation.¹¹⁴ Although

¹¹⁰ Pongó, 2018, p. 167.

¹¹¹ *#nemvagyegyedül* [Online]. Available at: <https://unicef.hu/nemvagyegyedul-2020>.

¹¹² *Kampány a Nők Lapjával az internetes zaklatás ellen*, 2020.

¹¹³ *1,5 millió megtekintést ért el két hét alatt a cyberbullying elleni TikTok kampányunk*, 2021.

¹¹⁴ *Az Internet Hotline szolgálatáról* [Online]. Available at: https://nmhh.hu/cikk/190105/Mi_az_Internet_Hotline

the term ‘bullying’ is used here instead of ‘harassment’, it is possible to mean such behaviour. However, this has hardly been a breakthrough: according to published statistics, although the number of reports of ‘online harassment’ has tripled between 2011 and 2021, this still only represents 114 cases, or 3% of all cases.¹¹⁵

In 2011, the *Safer Internet Hotline* was launched with the support of the European Union under the Safer Internet Plus program, which also provides a way to report online crime.¹¹⁶ According to its own website, the Hotline has the following tools in cases of cyberbullying:

- examine content;
- collect and store information to assist the police in their work;
- informing victims of possible and necessary legal action.

Information on the effectiveness of the operation is not available on the Hotline’s website, and the organisation has not communicated on its Facebook page since 2021.

It is also worth mentioning the *Blue Line Children’s Crisis Foundation*,¹¹⁷ which has been operating since 1993 and runs a *permanent hotline for psychological support* on 116-111. According to their website, they receive more than 21,000 calls per week. They also have the possibility to communicate via email and chat, which has also been used in thousands of cases. The main purpose of the line is not to provide concrete help, although there have been dozens of cases alike, but to provide spiritual support and talk through problems.

5. Responsibility of Service Providers

In Hungary, the liability of service providers was governed for a long time by the rules adopted by the European Union, especially by the so-called E-commerce Directive.¹¹⁸ In Hungary, the regulation was transposed into Act CVIII of 2001 (hereinafter: E-commerce Act).

¹¹⁵ *Vedd észre a red flageket, merj nemet mondani! – a Safer Internet Day kapcsán indít kampányt az NMHH*, 2022.

¹¹⁶ *Biztonságosinternet Hotline* [Online]. Available at: <https://www.biztonsagosinternet.hu/>

¹¹⁷ *Kék Vonal Gyermekkrízis Alapítvány* [Online]. Available at: <https://kek-vonal.hu/>

¹¹⁸ 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, OJ L 178, 17.7.2000., p. 1–16.

The issue of liability for content providers is more or less clear, they are liable for the content they publish under the Criminal Code,¹¹⁹ and for damages under the Civil Code.¹²⁰ However, intermediary service providers were exempt from liability if certain general rules apply. They were not obliged to actively monitor and filter the information they transmit, nor are they responsible for deciding on its lawfulness, under the terms of recitals 30–31 of Directive 2009/136/EC.¹²¹

There are, however, legal grey areas, such as comment sections, which may also be sites of cyberbullying. In Hungary, CC Decision no. 19/2014. (V. 30.) addressed the issue, concluding with a particular logic, that the content provider is liable for the comment section, even if the scope is rather narrow (in practice, it only covers online news portals). The case continued before the European Court of Human Rights, which in 2016, somewhat contradicting its own earlier jurisprudence, ruled that since the Hungarian Association of Content Providers involved in the case did not profit from the comments and the comments did not reach the level of incitement to action, it could not be held liable for their content.¹²² However, this hardly provides practical guidance for similar cases.

5.1. A New Dawn – Liability of Service Providers Since DSA

The regulation adopted by the European Union usually referred to as Digital Services Act (hereinafter: DSA)¹²³ brought the liability regime regarding intermediary service providers to a whole new level. As the book chapter related to the regulation of the European Union describes in detail its content, here we just highlight the fact that a reference to the newly established common rules on liability and possible grounds for exemption have been placed in Article 7 of the E-commerce Act.

¹¹⁹ In contrast, the Hungarian legislation is not entirely clear regarding the role of service providers in criminal proceedings either. For more details, see: Sorbán, 2019, pp. 84–101.

¹²⁰ Here we must also mention Act LIII of 2018 on the protection of private life, which also refers back to the rules on personality rights of the Civil Code. Arts. 12–13 of Act LIII of 2018. On the analysis of this Act, see: Halász, 2023, pp. 135–143.

¹²¹ Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009 amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, OJ L 337, 18.12.2009, p. 11–36.

¹²² Dornfeld, 2018, pp. 106–107.

¹²³ 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), OJ L 277, 27.10.2022, p. 1–102.

Although content monitoring is still not an obligation under the general rules, DSA promotes the cooperation between Member States and actors of the digital market. In the area, self-regulation is still of fundamental importance these days. Bill T/9996., which also aims to introduce a new criminal offence already discussed in Subchapter 2, contains a future amendment for Act CIV of 2010 on the freedom of press and fundamental rules on media content. According to the text, if the publisher of an online press product provides for the possibility of reader comments on the content of the press product on the internet platform it edits or on an online platform operated by others, *it must draw up a policy* on the procedure to control the publication of the unlawful comments and implement an effective solution accordingly. The publisher of an Internet press product shall make the rules publicly available. In other words, the bill aims to force service providers to create a regulation and practice on a control procedure similar to monitoring.

Summary

Hungarian legislation is quite abundant compared to other European countries. On the other hand, we shall conclude that the national legal system is not ready at this point to handle all the threats concerning the right to human dignity and other fundamental rights appearing in the online sphere. The analysed offences have proven that criminal law lacks specific tools in the fight against cyberbullying currently, but the new prohibition on aggression on Internet, yet to be adopted, shows the commitment of the legislator to improve in this field. In contrast, we must emphasise that in terms of best practices and research activity, Hungary is on its way to establish a system that focuses on prevention rather than sanctioning. The most apparent deficiency is the lack of well-established liability rules regarding service providers. In this regard, classic legal tools can be used. On the other hand, the idea of promotion of self-regulation on content control seems quite promising.

At this point, there are more questions than answers. New solutions appear in Hungarian legislation, partially thanks to the European harmonisation process. Nevertheless, though these novelties create an adequate basis for a better (online) world, practitioners will have the duty to chisel the content of the regulative framework during the next years.

Bibliography

- Ádám, A. (1990) *Magyar államjog*. Pécs: Pécsi Janus Pannonius Egyetem Állam- és Jogtudományi Kar.
- Barzó, T. (2018) 'Személyiségvédelem' in Barzó, T., Papp, T. (eds.) *Civilisztika I. Általános tanok – Személyek joga – Szellemi alkotások joga*. Budapest: Dialóg Campus, pp. 171–266.
- Bérces, V. (2017) 'A zaklatás törvényi tényállásába ütköző cselekmények minősítése és bizonyítási kérdései', *Magyar Jog*, 64(7–8), pp. 454–462.
- Bihari, O. (1983) *Korszerű tendenciák az államhatalom gyakorlásában*. Budapest: Közgazdasági és Jogi Könyvkiadó.
- Bihari, O. (1984) *Államjog – Alkotmányjog*. Budapest: Tankönyvkiadó.
- Csemáné Váradi, E. (2023) 'Az alternatív technikák mint az áldozati jogok gyakorlásának támogatói', *Fontes Iuris*, 9(1), pp. 26–33; <https://doi.org/10.51784/FI.2023.1.4>.
- Csink, L., Csink, L. (2024) 'A vallási érzékenységet sértő karikatúrák megítélése', *In Medias Res*, 13(1), pp. 5–21; <https://doi.org/10.59851/imr.13.1.1>.
- Domokos, A. (2022) 'Gyermekáldozatok védelme az online világban' in Homicskó, Á. O. (ed.) *A technológia fejlődés társadalmi kihívásai és hatása a jogi szabályozásra*. Budapest: Károli Gáspár University of the Reformed Church, pp. 71–88.
- Dornfeld, L. (2018) 'A közvetítő szolgáltatók felelőssége az internetes tartalmakért', *Kriminológiai Közlemények*, 2018/78, pp. 101–117.
- Erdős, Cs. (2021) 'Az alapjogok korlátozása' in Bódi, S., Schweitzer, G. (eds.) *Alapjogok: Az emberi jogok alkotmányos védelme Magyarországon*. Budapest: Ludovika, pp. 79–89.
- Figula, E. (2004) *Iskolai zaklatás – iskolai erőszak pszichológusszemmel*. Nyíregyháza: Szabolcs-Szatmár-Bereg Megyei Tudományos Közalapítvány.
- Gárdos-Orosz, F. (2018) 'Alapvető jogok korlátozása' in Lamm, V. (ed.) *Emberi jogi enciklopédia*. Budapest: HVG-Orac, pp. 26–32.
- Gárdos-Orosz, F. (2021) '30/1992 (V. 26.) AB határozat – gyűlöletbeszéd' in Gárdos-Orosz, F., Zakariás, K. (eds.) *Az Alkotmánybírósági gyakorlat: Az Alkotmánybíróság 100 elvi jelentőségű határozata Part I*. Budapest: Társadalomtudományi Kutatóközpont, HVG-Orac, pp. 203–219.
- Gosztonyi, G. (2020) 'A parlamentrizmus helyreállítása' in Mezey, B., Gosztonyi, G. (eds.) *Magyar alkotmánytörténet*. Budapest: Osiris, pp. 505–520.
- Halász, Cs. (2023) *A magánélethez való jog*. Miskolc: Bíbor.
- Holló, A. (1997) *Az alkotmányvédelem kialakulása Magyarországon: Az Alkotmányjogi Tanácstól az Alkotmánybíróságig*. Miskolc: Bíbor.

- Horváth, A. (2023) 'Az alkotmánybíráskodás jogtörténeti előzményei Magyarországon' in Veress, E., Fegyveresi, Zs. (eds.) *Liber amicorum Attila Varga. Tisztelgő kötet Varga Attila 60. születésnapjára*. Kolozsvár: Forum Iuris, pp. 71–103.
- Horváth, A., Völgyesi, L. (2020) 'A szovjet típusú totális diktatúra Magyarországon' in Mezey, B., Gosztonyi, G. (eds.) *Magyar alkotmánytörténet*. Budapest: Osiris, pp. 492–501.
- Huszár, J. (2022) 'Emberkereskedelem újragondolva – a 2020. július 1-jén hatályba lépett rendelkezések hatékonysága ügyési szemmel', *Belügyi Szemle*, 70(2), pp. 305–325.
- Jakab, A. (2020) 'Mit tehet az alkotmányjog a demokrácia és a jogállamiság eróziója ellen? A demokrácia és a jogállamiság védelmének elválaszthatatlanságáról', *Állam- és Jogtudomány*, 61(3), pp. 74–96.
- Jármí, É. (2019) 'Az iskolai bántalmazás (bullying) megelőzése', *Educatio*, 28(3), pp. 528–540; <https://doi.org/10.1556/2063.28.2019.3.6>.
- Jármí, É., Péter-Szarka, Sz., Fehérpataky, B. (2015) *A KiVa-program hazai adaptálásának lehetőségei*. Budapest: Institute for Educational Research and Development.
- Kiss, T. (2016) 'Internetes mémek mint káros információs egységek a tartalom-bűncselekmények körében' in Fazekas M. (ed.) *Jogi tanulmányok*. Budapest: Eötvös Loránd University, pp. 350–360.
- Kissné Viszket, M., Horgász, Cs. (2013) 'Békés iskolák projekt. Az iskolai agresszió megfékezése és megelőzése' in Kiss, E. Cs., Sz. Makó, H. (eds.) *Mentálhigiéné és segítő hivatás*. Pécs: Pannónia, pp. 262–280.
- Koi, Gy. (2005) 'Lehetséges értelmezési tartományok a közérdek köréből', *Állam- és Jogtudomány*, 46(1–2), pp. 77–106.
- Koi, Gy. (2023) 'Sólyom László (1942–2023)', *Állam- és Jogtudomány*, 64(3), pp. 91–98; <https://doi.org/10.51783/ajt.2023.3.09>.
- Koltay, A. (2013) 'A nagy magyar gyűlöletbeszéd-vita: a „gyűlöletre uszítás” alkotmányos mércéjének azonosítása felé', *Állam- és Jogtudomány*, 54(1–2), pp. 91–123.
- Koltay, A. (2021a) 'Constitutional Protection of Freedom of Expression in the First Decade of the Fundamental Law of Hungary', *Iustum Aequum Salutare*, 17(4), pp. 73–123; <https://doi.org/10.2139/ssrn.3978111>.
- Kovács, H. (2021) 'A vallási közösségek méltóságának sérelme az Alkotmánybíróság értékelésében személyiségi jogi területen', *In Medias Res*, 10(2), pp. 331–359.
- Kukorelli, I. (2017) 'Az 1946. évi I. törvény közjogtörténeti jelentősége és az alkotmányos jogfolytonosság', *Acta Humana*, 5(1), pp. 21–26.

- Kulcsár, G. (2024) *Bullying és cyberbullying. Hogyan előzzük meg és kezeljük az iskolai és az online kortársbántalmazást?* Budapest: Novissima.
- Mezőlaki, E. (2022) 'A köznyugalom elleni bűncselekmények: XXXII. fejezet' in Karsai, K. (ed.) *Nagykommentár a Büntető Törvénykönyvhöz*. Budapest: Wolters Kluwer, pp. 787–809.
- Monori, Zs. É. (2016) 'Zaklatás-e a cyberbullying? Az internetes zaklató magatartások büntetőjogi szankcionálásának dilemmái', *In Medias Res*, 5(1), pp. 246–261.
- Nagy, M. (2023) 'A köznyugalom elleni bűncselekmények' in Gál, I. L. (ed.) *Magyar büntetőjog – Különös rész*. Budapest: Osiris, pp. 342–360.
- Pap, G. (2013) 'Az alkotmányjog alapfogalmai' in Paulovics, A. (ed.) *Alkotmányjog bachelor szakos hallgatók számára*. Miskolc, Miskolci Egyetemi Kiadó, pp. 9–29.
- Parti, K. (2016) 'A megfélemlítés (bullying) szabályozása Magyarországon és külföldön', *In Medias Res*, 5(1), pp. 114–146.
- Paulovics, A. (2013) 'Az alapjogok rendszere' in Paulovics, A. (ed.) *Alkotmányjog bachelor szakos hallgatók számára*. Miskolc, Miskolci Egyetemi Kiadó, pp. 136–141.
- Pribula, L. (2023) 'Személyiségvédelem' in Jakab, A., Könczöl, M., Menyhárd, A. (eds.) *Internetes Jogtudományi Enciklopédia*. [Online]. Available at: <http://ijoten.hu/szocikk/szemelyisegvedelem>
- Sántha, F. (2020) 'A köznyugalom elleni bűncselekmények' in Görgényi, I., Gula, J., Horváth, T., Jacsó, J., Lévy, M., Sántha, F., Váradi, E. (eds.) *Magyar büntetőjog – Különös rész*. Budapest: Wolters Kluwer, pp. 578–601.
- Sári, J. (2004) *Alapjogok – Alkotmánytan II*. 3rd edn. Budapest: Osiris.
- Smuk, P. (2019) 'Az önkényuralmi rendszerek jelképei és a használatukat tiltó jogi szankciók rendszere', *In Medias Res*, 8(2), pp. 230–252.
- Sólyom, L. (2001) *Az alkotmánybíráskodás kezdetei Magyarországon*: Budapest: Osiris.
- Sólyom, P. (2021) 'Kelsen köpönyegéből. A magyar alkotmánybíráskodás keletkezéstörténetéhez', *Közjogi Szemle*, 14(2), pp. 1–17.
- Sorbán, K. (2019) 'Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában', *In Medias Res*, 8(2), pp. 84–101.
- Szomora, Zs. (2024) 'A köznyugalom elleni bűncselekmények (Btk. XXXII. fejezet)' in Karsai, K. (szerk.) *Anyagi büntetőjog – Különös rész*. Szeged, Iurisperitus, pp. 327–335.
- Trócsányi, L. (2014) *Az alkotmányozás dilemmái. Alkotmányos identitás és európai integráció*. Budapest: HVG-Orac.

- Vastagh, P. (2019) 'Egy "idegen test" a szocialista államszervezetben. Adalékok az Alkotmányjogi Tanács létrejöttének történetéhez', *Közjogi Szemle*, 12(1), pp. 46–59.
- Varga, Zs. A. (2015) *Eszményből bálvány? A joguralom dogmatikája*. Budapest: Századvég.
- Televele Médiapedagógiai Műhely Egyesület (2018) *A biztonságos internethasználat fejlesztése. Kortárs médiamentor program – Kézikönyv a képzéshez*. Budapest: Televele Médiapedagógiai Műhely Egyesület.
- TKKI (2017) *NyugiOvi Program – Kora-gyermekkori program a megfélemlítés megelőzésére. Kézikönyv óvodapedagógusok részére*. Budapest: TKKI.
- Tóth, J. Z. (2013) 'Önkényuralmi jelképek v. szólásszabadság – Az Alkotmánybíróság 4/2013. (II. 21.) AB határozata az önkényuralmi jelképek használatáról', *Ügyészek Lapja*, 2013/3–4, pp. 47–58.
- Tóth, J. Z. (2017) *A büntetőjogi rágalmozás és becsületsértés*. Budapest: NMHH Médiatudományi Intézet.
- Tóth, J. Z. (2020) *Demokrácia, jogállamiság és alkotmánybíráskodás*. Budapest: Patrocinium.
- Tóth, G. A. (2024) *Nemdemokrácia: Az alkotmányjogi patológia és terapia alapjai*. Budapest: Oriold és Társai.
- Virág, G., Parti, K., Schmidt, A., Néray, B. (2014) 'TABBY in Internet – Az online bántalmazások volumenének iskolai felmérése és mentorképzés Magyarországon (2010–2014)', *Ügyészek Lapja*, (3–4), pp. 47–58.
- 1,5 millió megtekintést ért el két hét alatt a cyberbullying elleni TikTok kampányunk (2021) UNICEF, 2 July [Online]. Available at: <https://unicef.hu/igy-segitunk/hireink/egyutt-a-serto-hangok-ellen-tiktok-kampany-eredmeny>
- Kampány a Nők Lapjával az internetes zaklatás ellen (2020) Hintalovon, 17 September [Online]. Available at: <https://hintalovon.hu/2020/09/17/kampany-az-internetes-zaklatas-ellen/>
- Vedd észre a red flageket, merj nemet mondani! – a Safer Internet Day kapcsán indít kampányt az NMHH (2022) NMHH, 7 February [Online]. Available at: https://nmhh.hu/cikk/226722/Vedd_eszre_a_red_flageket_merj_nemet_mondani__a_Safer_Internet_Day_kapcsan_indit_kampanyt_az_NMHH

VII. HATE SPEECH AND CYBERBULLYING IN CZECH LAW

DÁVID HOJNYÁK

1. Hate speech in Czech law

If we look for the constitutional basis of hate speech in the Czech legal order, we find that the constitutional legislation¹ does not contain *expressis verbis* provisions on this subject, while the *Charter of Fundamental Rights and Freedoms* (hereinafter: Charter) provides that freedom of expression and the right of access to and dissemination of may be restricted by law where this is necessary in a democratic society in order to protect the rights and freedoms of others, the security of the State, public security and public health, and public morals.² We see, therefore, that the Charter lays down a kind of limitation clause which allows for the restriction of these fundamental constitutional rights in certain circumstances, while taking into account the criteria of legality, necessity and proportionality.³ With regard to the constitutional basis of the legislation on this subject, it is also worth noting the Charter's provisions on human dignity⁴, the protection of privacy⁵, and the protection of personal data.⁶

Provisions on hate speech can be found in Czech legislation in the context of criminal law, although it should be noted that the term hate speech is not

1 It is important to note that the Czech constitutional order consists of the Constitution, the Charter of Fundamental Rights and Freedoms and a set of so-called constitutional laws (also known as constitutional laws or constitutional enactments).

2 Article 17 para. (4) of the Charter

3 For more information on the characteristics of these fundamental constitutional rights and the detailed rules for their limitation, see Bartoň and Hejč, 2021, and Herczeg, 2004, pp. 85-86.

4 Articles 1 and 10 para. (1) of the Charter.

5 Articles 7 and 10 para. (2) of the Charter.

6 Article 10 para. (3) of the Charter.

recognised in Czech law. The Czech Criminal Code (Act No 40/2009, hereinafter referred to as ‘the Criminal Code’)⁷ lists the relevant offences in Chapter 10, which contains offences against public order (including offences against human coexistence), and in Chapter 13, which contains offences against humanity and peace and war crimes (including offences against humanity). The Criminal Code therefore contains several elements that correspond to the category of hate speech or have a close connection with it, which are briefly analysed below.

1.1. Defamation of a national, racial, ethnic or other group of persons

The first provision of the Criminal Code relevant to the topic under consideration is Article 355, which is entitled “Defamation of *national, racial, ethnic or other groups of persons*.”⁸ According to this provision, if a person publicly defames a nation and its language, a race, an ethnic group or a group of persons on the grounds of their actual or perceived race, ethnic group, nationality, political opinion, religion or actual or perceived atheism, he commits the offence.⁹ The qualified case of this offence is also relevant to the subject under consideration, whereby the offender is punished more severely if he commits the offence through the media, films, radio, television, publicly accessible computer networks or other similar means.¹⁰

1.2. Incitement to hatred against a group of persons or incitement to restrict their rights and freedoms

Another form of hate speech is defined in the Article 356 of the Criminal Code, which is called “*Incitement to hatred or to restriction of the rights and freedoms of a group of persons*”.¹¹ According to the definition of the Penal Code, whoever publicly incites hatred against a national, racial or ethnic group, religious community, social class or other group of persons, or incites the restriction of the rights and freedoms of members of such communities, commits the offence.¹² The law also provides for the punishment of anyone who attempts or conspires to commit such an act.¹³ The Penal Code defines as a qualified case, similar

⁷ The Criminal Code is available at the following link: <https://www.zakonyprolidi.cz/cs/2009-40>

⁸ In Czech: “*Hanobení národa, rasy, etnické nebo jiné skupiny osob*”.

⁹ Criminal Code 355 § para. (1)

¹⁰ Criminal Code 355 § para. (2)

¹¹ In Czech: “*Podněcování k nenávisti vůči skupině osob nebo k omezování jejich práv a svobod*”.

¹² Criminal Code 356 § para. (1)

¹³ Criminal Code 356 § para. (2)

to the one discussed above, when the offender commits the offence through a press product, film, radio, television, a publicly accessible computer network or other similar means, and when the offender actively participates in the activities of a group, organisation or association that promotes discrimination, violence or incites hatred against a race, ethnicity, social class, religious group or other group of persons.¹⁴

1.3. Violence against a group of people and an individual

Another provision of the Criminal Code should be mentioned in connection with the category of hate speech, namely the provision in Article 352, which is called “*Violence against a group of people and an individual*”.¹⁵ According to the basic case, if a person threatens a group of residents with death, bodily harm or substantial damage, he or she has committed the offence covered by the Act. The Criminal Code defines as a qualifying case in comparison with the basic case the offender who uses violence against a group of the population or a person, or threatens that group of persons with death, bodily harm or substantial damage because of his or her actual or perceived race, ethnicity, nationality, political opinion, religion or even his or her actual or perceived atheism.¹⁶ In the case of this offence, we see that the basic offence is not explicitly linked to the category of hate speech, but the aggravated offence is, since the offence is committed by threatening death, bodily harm or substantial damage- against a specific group of persons. Under the Criminal Code, the commission of such an offence by means of a press product, film, radio, television, a publicly accessible computer network or other similar means, as well as the attempt or conspiracy to commit such an act, is a qualified case in comparison with the basic case.¹⁷

1.4. Other offences

It is also necessary to mention the criminal offences of the Criminal Code concerning the creation, support and promotion of a movement for the suppression of human rights and freedoms or the promotion of hatred against racial, ethnic, national, religious or class hatred or against any other group of persons

14 Criminal Code 356 § para. (3)

15 In Czech: „*Násilí proti skupině obyvatelů a proti jednotlivci*”.

16 Criminal Code 352 § para. (1)

17 Criminal Code 352 § para. (2)-(3)

(403 §),¹⁸ the dissemination of a work promoting such a movement (403a §),¹⁹ and the public expression of sympathy for such a movement (404 §).²⁰

Closely related to hate speech is the offence of approving the commission of a crime (365 §)²¹ on the one hand, and the offence of publicly denying, questioning, approving or justifying genocide (405 §)²² on the other. The former offence is committed by anyone who publicly approves of a crime committed or publicly praises the perpetrator of the crime for having committed it. This offence may be of particular interest in the context of the shooting at Charles University in Prague in December 2023,²³ where comments under internet articles reporting the massacre, identifying with the event and the perpetrator, and praising the act and the perpetrator itself, constituted the offence as defined by the law. As regards the latter offence, it is worth mentioning at this point the official statement by the Prosecutor General on the Russian-Ukrainian conflict. The Prosecutor General's statement of 26 February 2022, entitled "*Information on the possible criminal limitations of freedom of expression in relation to the situation in Ukraine*", states that, although Czech constitutional rules declare freedom of expression, it has its limits. This means, in the context of the Russia-Ukraine war, according to the Prosecutor General's statement, that if a person expresses publicly (including at demonstrations, on the Internet or other social networks) his or her approval of (i.e. acceptance or support for) Russia's aggression against Ukraine, or in this context expresses support or praise for the leaders of the Russian state, he or she may, under certain conditions, be held criminally liable under the Criminal Code 365 § (i.e. approval of the crime) and 405 § (i.e. public denial, questioning, approval or justification of genocide is a criminal offence) of the Russian Federation.²⁴

It is also interesting to note that the Penal Code lists in a taxative manner the circumstances that the court must take into account as aggravating circumstances in sentencing for each offence. On this basis, the Code classifies as an aggravating circumstance, among others, the fact that the offender commits

18 In Czech: „Založení, podpora a propagace hnutí směřujícího k potlačení práv a svobod člověka”.

19 In Czech: „Šíření díla k propagaci hnutí směřujícího k potlačení práv a svobod člověka”.

20 In Czech: „Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka”.

21 In Czech: „Schvalování trestného činu”.

22 In Czech: „Popírání, zpochybňování, schvalování a ospravedlňování genocidia”.

23 On 21 December 2023, a 24-year-old student at Charles University in Prague opened fire in the main building of the Faculty of Arts in the city centre. He planned the shooting in advance. During the massacre, he killed fourteen people and eventually killed himself.

24 The Attorney General's statement is available via the following link: <https://verejnazaloba.cz/nsz/informace-k-moznym-trestnepravnim-limitum-svobody-projevu-ve-vztahu-k-situaci-na-ukrajine/>

VII. HATE SPEECH AND CYBERBULLYING IN CZECH LAW

the offence (e.g. murder) because of hatred against a national, racial, ethnic, religious or social class.²⁵

In summary, Czech national law criminalises and punishes certain forms of hate speech in the form of the above²⁶ offences, although it does not recognise the term hate speech itself.²⁷ The table below provides a clear overview of the groups at risk and the types of conduct that can be committed in relation to each of the legal offences of hate speech.

Name of the offence	Criminal Code provision	Vulnerable group	Compliance behaviour
Violence against a group of people and an individual	352. § para. (2)-(3)	a group that can be separated on the basis of national, racial, ethnic, religious or political opinion	threat
Defamation of a national, racial, ethnic or other group of persons	355. §	a group that can be separated on the basis of national, racial, ethnic, religious or political opinion	public defamation
Incitement to hatred against a group of persons or incitement to restrict their rights and freedoms	356. §	a national, racial, ethnic, religious, social class or other group of persons	publicly inciting hatred, incitement
To create, support and promote a movement to suppress human rights and freedoms	403. §	any group of persons (at the same time, the Criminal Code names the racial, ethnic, national, religious and social class against which the activity of such a movement may be directed)	creating, supporting and promoting a hate movement

²⁵ Criminal Code 42 § point (b)

²⁶ For a more detailed analysis of the facts analysed, see Nováková, 2010, pp. 7-11, pp. 16-21, and Strakoš, 2021, pp. 9-13.

²⁷ At this point, it is worth mentioning that the most comprehensive European treaty protecting the rights of persons belonging to national minorities, the *Framework Convention for the Protection of National Minorities*, under the control of the Committee of Ministers of the Council of Europe, highlighted in its latest report on the Czech Republic in 2021, that, although the Czech Republic has recently made some progress in the fight against discrimination, the report also called on the Czech authorities to step up their efforts to combat stereotypes and prejudice against minority groups most vulnerable to hate speech, among other things by effectively prosecuting cases of criminal relevance (Report, 6. The report is available via the following link: <https://rm.coe.int/5th-op-czech-republic-en-restricted/1680a2b3d6>).

Name of the offence	Criminal Code provision	Vulnerable group	Compliance behaviour
Distribution of works promoting the movement to suppress human rights and freedoms	403a §	see the provisions of 403 §	producing, importing, exporting, transporting, offering, making available to the public, transmitting, marketing, selling, selling or otherwise transferring such works (in particular emblems, flags, logos, etc.) in large quantities, or creating such works for others
Expressing sympathy for the movement to suppress human rights and freedoms	404. §	see the provisions of 403. §	public expression of sympathy
Public denial, questioning, approval or justification of genocide	405. §	not relevant	public denial, questioning, approval, confirmation

Table 1: Legal elements constituting hate speech in the Czech Criminal Code

The table shows that the common feature of the offences analysed is that the groups at risk are broadly the same, i.e. such offences are specifically directed against a national, racial, ethnic, religious group or a group that can be distinguished on the basis of political opinion. The range of offences takes four main forms: defamation, incitement to hatred (and certain forms of conduct linked to a movement carrying out such activities), incitement and threats. After analysing the constituent elements, it can also be concluded that hate speech conduct can be committed both offline and online, and that the constituent elements (with the exception of those in Articles 404 and 405) consider as a qualifying case when the offender commits an offence through a press product, film, radio, television, a publicly accessible computer network or other similar means.

At the same time, the question arises as to where the boundaries of freedom of expression can be drawn in practice, in the application of the law by the judiciary, i.e. how broadly or narrowly the above-mentioned definitions of hate speech can be interpreted. A relatively recent decision of the Czech Constitutional Court from December 2021, which deals in part with this question, may help us to answer this question. The decision was based on the following case: a picture of first-graders at a primary school in Teplice in north-western Bohemia, in which a significant number of the children are of Arab and Roma origin. The picture was posted on Facebook, with *Vítězslav Kroupa* commenting: “*It’s a good thing they go to the Plynárenská [Gas Factory] Street Primary School. The solution is obvious.*” The

criminal proceedings against the commentator were opened on the basis of two offences: firstly, the criminal offence under the Article 356 of the Criminal Code, which, as analysed above, is known as “*Incitement to hatred or restriction of the rights and freedoms of a group of persons*”, and on the other hand, the offence of “*incitement to hatred or restriction of the rights and freedoms of a group of persons*”. Article 404,²⁸ which makes it a punishable offence to express sympathy for a movement or idea that aims to suppress human rights and freedoms – in this case, this idea is obviously Nazism. Before the case was brought before the Constitutional Court, it went through several judicial forums. At this point, we will only highlight some details from the decision of the Supreme Court.²⁹ According to the Supreme Court, Kroupa’s comment was clearly a reference to the extermination of ‘*undesirable ethnicities*’ in gas chambers, i.e. that children of Arab and Roma origin in the picture should be treated in the same way as the Nazis systematically murdered people of Jewish origin and others during the Second World War. “*In a state governed by the rule of law, based on respect for constitutionally guaranteed civil and human rights, such remarks are unacceptable and must be responded to by the means of criminal law*”- says the Supreme Court decision.³⁰ The defence, however, argued that Kroupa’s comment was merely black humour and an opinion that was within the bounds of freedom of expression, but the argument was not found credible by the Supreme Court, which rejected it. In its decision, the Court also stated that “*the expression of certain values or opinions is not and cannot be a criminal offence. On the other hand, public incitement to hatred or expressing sympathy for hate movements is punishable under the conditions laid down in the Criminal Code.*”³¹ It should be noted that Kroupa has previously been convicted of posting a picture of an imperial eagle holding a Nazi swastika, as well as a portrait of convicted Nazi war criminal Hermann Göring and Adolf Hitler on social media, so it was obvious to the court at the time of the case that the commentator was sympathetic to Nazi ideas. The case was subsequently brought to the Constitutional Court by Kroupa through a constitutional complaint. In its decision³², the Constitutional Court in fact confirmed the decision and reasoning of the Supreme Court and the lower courts that had previously ruled that Kroupa’s commentary could not be considered black humour and was

28 In Czech: „*Projev sympatií k hnutí směřujícímu k potlačení práv a svobod člověka*“.

29 The Supreme Court’s decision 564/2021 [3 Tdo 564/2021 Usnesení NS ze dne 24.06.2021, hereinafter: SC decision] is available via the following link: <https://www.zakonyprolidi.cz/judikat/nscr/3-tdo-564-2021>

30 SC Decision, Reasoning, point 70.

31 SC Decision, Reasoning, point 74.

32 The decision of the Constitutional Court [III.ÚS 2696/21 ze dne 7. 12. 2021, hereinafter: CC decision] is available via the following link: https://nalus.usoud.cz/Search/GetText.aspx?sz=3-2696-21_1

not protected by the fundamental constitutional right of freedom of expression, and therefore should be considered as hate speech – on the internet- as a form of hate speech, which in a democratic society must be combated by criminal law.³³ The Constitutional Court therefore dismissed the constitutional complaint and sentenced Vítězslav Kroupa to 16 months' imprisonment, suspended for three years.³⁴ In conclusion, in the Czech Republic, judicial practice already classifies as hate speech the expression of an opinion or value judgement that incites hatred against a specific group or group of persons by means of a comment on a post on a social media platform, in this case Facebook. We can therefore see that, on the basis of Czech case-law, the fundamental constitutional right to freedom of expression is not absolute.

2. Regulation of (cyber)bullying in Czech law

Czech law does not recognise the categories of *bullying* and *cyberbullying*, so they are not defined as separate facts in the Criminal Code or other legislation.³⁵ However, the Czech Penal Code contains a number of provisions which contain elements of one or other of these categories. Accordingly, the following is a brief description of those elements of the Criminal Code which, in terms of content, correspond most closely to the instrumental acts or a manifestation of the categories of bullying and cyberbullying.

However, before proceeding to the analysis outlined above, it is necessary to briefly refer to the public law, or more precisely the constitutional law, basis of the issue of cyberbullying. As we shall see, some forms of cyberbullying always involve a negative intrusion into the privacy and daily life of the victim. Accordingly, it is necessary to refer to Article 10 para. (2) of the Charter as the constitutional basis for the Czech legislation, which declares that everyone has the right to be protected against unlawful interference with private and family life.³⁶

2.1. Concepts of cyberbullying in Czech criminal law

The Czech Criminal Code contains five elements that can be linked and applied to acts of cyberbullying. These are analysed below, together with a brief

³³ CC Decision, Reasoning, point 11

³⁴ CC Decision, Reasoning, point 12

³⁵ Cf. Parti, 2016, 117, and Vištalová, 2021, p. 1 and p. 24.

³⁶ Vištalová, 2021, pp. 14-16.

reference to those elements of the case law which are of great relevance to the topic.

2.1.1. Breach of confidentiality of forwarded messages

The first relevant offence in Chapter 2 of the Penal Code is the violation of the confidentiality of transmitted messages (*porušení tajemství dopravovaných zpráv*, hereinafter referred to as ‘breach of secrecy’), which is a violation of the rights of personality, privacy and confidentiality of correspondence. This offence is in fact a violation of the right to privacy by obtaining and/or disclosing personal data without authorisation.³⁷ In the context of cyberbullying, the first two paragraphs of the offence are relevant. On the one hand, according to the Criminal Code, anyone who intentionally:

- a) the secrecy of any data, text, voice or image message sent over an electronic communications network and addressed to an identified participant or user receiving the message; or
- b) breaches the confidentiality of non-public transmissions of computer data to, from or within a computer system commits this offence.³⁸

On the other hand, the Penal Code also specifies the scope of cases where a person discloses or uses a secret which he or she has learned through correspondence, telegrams, telephone calls or transmission via electronic communications networks, with the intention of causing damage to another person or of obtaining unlawful gain for himself or herself or for another person.³⁹

Comparing these facts with the traditional conceptual elements of cyberbullying, we can say that there is a weak correspondence between the two categories, since although the perpetrator commits the breach of confidentiality intentionally, there is no continuity, regularity or subordination between the parties. A further important difference between the two categories is that in the case of a breach of secrecy, the fear of intimidation is not the aim of the perpetrator’s actions, but only a potential result.

³⁷ If we have already mentioned the constitutional foundations of this issue above, in the context of this offence, we can mention, in addition to Article 20(2) of the Charter, the provisions of Article 20(3) of the Charter, which states that everyone has the right to be protected against the unlawful collection, disclosure or other misuse of personal data concerning him or her.

³⁸ Criminal Code 182 § para. (1) points (b)-(c)

³⁹ Criminal Code 182 § para. (2)

2.1.2. Defamation

The Criminal Code also provides for the next relevant offence, defamation (*pomluva*), in the area of violation of the rights of personality, privacy and confidentiality of correspondence. of the Czech Penal Code, a person who makes an untrue statement about another person which is likely to seriously damage the reputation of that person in the eyes of others (in particular if it causes damage to his employment, or interferes with his family relations, or causes him other serious harm) commits the offence of defamation.⁴⁰ It can be seen that this statutory element can only be linked to bullying in a very indirect way, since it lacks a relationship of subordination between the parties, a repetitive character (i.e. regularity and continuity) and, thirdly, it is seen that bullying can take the form of a result of defamation and not an explicit objective. The link of defamation to cyberbullying may be based on the qualified case of this offence. According to this provision, where the offender commits defamation in the press, on film, radio, television, via a publicly accessible computer network or by other similar means, the offence is punishable more severely than in the main case.⁴¹ This leads to the conclusion that there is also a weak correlation between defamation and cyberbullying, in other words, that defamation is on the borderline of cyberbullying.

2.1.3. Blackmail with sexual intent

Perhaps the most interesting element of the Czech legislation in this respect is the sexual blackmail (*sexuální nátlak*), which is a special type of bullying and is defined as a separate offence in the Criminal Code. In the context of the historical development of this offence, it should be noted that this specific form of blackmail is a new offence in the current Criminal Code, which the legislator has included in the category of sexual offences against human dignity. It is only partly new because, although it takes over certain provisions of the previous Criminal Code, other elements of the offence are completely new.⁴² The primary reason for including the new provisions and twists in the Penal Code was to respond to a regulatory loophole, since the previous legislation did not allow

40 Criminal Code 184 § para. (1). Article 20 para. (1) of the Charter declares that everyone has the right to respect for human dignity, honour, reputation and the protection of his or her name.

41 Criminal Code 184 § para. (2)

42 An example of this is the element of the legislation that previously applied only to persons under the age of 18, as opposed to the current legislation, which now applies to all persons regardless of age. It is a different matter that the current Penal Code provides for more severe penalties in cases where the offence is committed against a minor.

for the criminalisation of certain acts, which were, however, relatively often committed in practice.⁴³ It should also be noted that this form of extortion is a subsidiary offence, since it can only be established if the offence of rape referred to in Article 185 of the Criminal Code is not committed.

Compared to the classic case of extortion, this is a special case because the perpetrator forces the victim to perform a sexual act (in most cases this means masturbation and stimulation of the genitals or other erogenous zones with hands, erotic aids or other objects)⁴⁴, to take nude or poorly dressed photographs or to perform other similar acts, while the perpetrator blackmails the victim by publishing a sexually explicit recording (picture or video) in his possession.⁴⁵ The offence is defined in the Criminal Code as follows: whoever coerces another person to perform a sexual act, to take nude or poorly clothed photographs or other similar acts, or who coerces another person to perform such acts by exploiting his vulnerability, by using violence, threats of violence or other serious harm, commits the offence of extortion for the purpose of sexual exploitation.⁴⁶ The phrase '*coerces another to commit a similar act*' requires some explanation, as the interpretation of this phrase is problematic for jurisprudence and case-law. It covers any behaviour that may be similarly humiliating for the victim, such as sexual self-disclosure or exposure. Therefore, for example, the offence may take the form of coercion to use sexual gestures or vocal expressions intended to arouse the sexual arousal of the offender or to increase it.⁴⁷ As can be seen, although the facts of the case do not presuppose a relationship of subordination between the parties, it may nevertheless be a qualifying circumstance. It should be noted that, in addition to a relationship of subordination, the Czech Criminal Code considers as a qualifying circumstance the offender's use of the victim's dependency (addiction); his use of a child; his use of weapons or a group of persons to injure several persons; and his causing serious bodily injury or death to the victim.⁴⁸ The Criminal Code also criminalises preparation.⁴⁹ It can also be seen that bullying can be a result of the offence, not a condition of it, and that repeated or continuous bullying is not mentioned in the offence, i.e. the conceptual elements of bullying cannot be fully identified with those in the offence.

43 Holas, 2012, p. 24.

44 Fremr, 2015, pp. 1017-1018.

45 Cf.: Party, 2016, pp. 126-127.

46 Criminal Code 186 § para. (1).

47 Ščerba, 2009, pp. 546-549.

48 Criminal Code 186 § para. (2)-(6).

49 Criminal Code 186 § para. (7).

Despite the differences, we would like to highlight the link between sexual harassment and cyberbullying by briefly presenting a case. In the case, a middle-aged man, *Patrik Krajíček*, contacted 19 underage girls (some of the victims were under 15 at the time of the offence) between 2017 and 2020 via Facebook under a pseudonym and with a pseudo-profile in order to extort sexual photos and videos from them. In the majority of cases, the perpetrator was successful, promising money or gifts in exchange for the photos and videos. However, after a while, when the victims tried to stop communicating with the man or refused to respond to his requests, the perpetrator would threaten them, most often by making public the intimate photos and videos they had already sent, and in rare cases by threatening them with violence. The perpetrator said that he did not intentionally contact minors, nor did he intend to meet the victims in person. On this basis, the offender was prosecuted for *sexual harassment*. The court finally imposed a sentence of three years' imprisonment (suspended for five years) and a fine, and ordered him to refrain from communicating electronically or in writing with anyone under the age of 18 for the duration of the sentence.⁵⁰ This case shows that the Czech case-law applies the concept of sexual harassment to certain cases of online abuse. This raises the possibility that the same concept could be applied in the future to specific cases of cyberbullying between peers, including sexual blackmail.

2.1.4. *Dangerous threat*

The Czech Penal Code's definition of dangerous threat (*nebezpečné vyhrožování*, hereinafter 'threat') also has some similarities with the category of bullying. The Penal Code mentions threats in Chapter 10, which covers offences against public order, including offences that disturb human coexistence. According to this definition, a person who threatens another person with death, grievous bodily harm or other serious harm in a way that is likely to cause fear in the other person, is deemed to have committed the offence covered by the Act.⁵¹ In this case, we can see that the primary aim and intention of the perpetrator is to create fear, and in this form it is similar to bullying, but in the case of threats there is no shift in the balance of power compared to bullying, nor is there any element of repetition or continuity in the facts under examination. The relevant literature states that the offence does not require the personal presence of the person to whom the threat is addressed, i.e. it is sufficient for the offence to be committed if the

50 The case summary is based on the following article: <https://www.ceskenoviny.cz/zpravy/za-sexualni-natlak-vuci-nezletilym-ulozil-soud-muzi-z-luhacovic-podminku/2232595>

51 Criminal Code 353 § para. (1).

addressee becomes aware of it, for example by telephone or electronic means of communication.⁵² This latter finding confirms that the threat can be linked to the category of cyberbullying.

2.1.5. *Dangerous harassment*

The legal definition of dangerous harassment (*nebezpečné pronásledování*, hereinafter: harassment) also shows some similarity with the category of intimidation, which, like threats, is also included in the Criminal Code in the category of offences that disturb human coexistence. With regard to cyberbullying, the two aspects of the offence should be highlighted, namely that harassment may be committed by means of persistent contact with the victim by electronic means, in writing or by other means, or by misusing the victim's personal data for the purpose of personal or other contact, and that such conduct is likely to cause the victim to fear for his or her life or health or that of persons close to him or her.⁵³ In the context of harassment, the intimidation as an intent or the act itself is of a long duration (continuous, persistent or repeated). The latter raises the question of how we should interpret the notion of persistence of harassing conduct over a long period of time. A 2011 decision of the Supreme Court⁵⁴ helps us to answer this question. In its decision, the Supreme Court stated that, for this offence, a long duration of harassment means repeated violent contact or attempts by the perpetrator with the victim (i.e. an isolated or random act does not meet this requirement), which must also be capable of creating real fear in the victim. Accordingly, the consistent, persistent, persistent and systematic actions of the perpetrator may constitute conduct which gives rise to the offence. However, the relevant literature goes further by stating that repetition occurs when the offender makes more than 10 attempts to contact the victim and these attempts take place over a period of at least 4 weeks.⁵⁵ The Decision also underlines that in the case of this offence, the offender's behaviour typically deviates from normal norms of behaviour and may therefore in some

⁵² Shamal, 2012, p. 3000.

⁵³ Criminal Code 354 § para. (1) points (c) and (e).

⁵⁴ Decision 1082/2011 of the Supreme Court of Justice [8 Tdo 1082/2011 Usnesení NS ze dne 08.09.2011]. The decision is available via the following link: <http://kraken.slv.cz/8Tdo1082/2011>

⁵⁵ Šámal, 2012, p. 3295. It should be noted that the case law has accepted and adopted this interpretation of the legal literature, as it has referred to this interpretation in several decisions. See, for example, the reasoning of Supreme Court decisions 1625/2016 and 777/2018.

cases be dangerous for the victim. However, in a 2013 decision⁵⁶, the Supreme Court also addressed the question of what constitutes an act of harassment that results in harassment by electronic means. In particular, the case-law considers that this includes the regular sending of unsolicited e-mails (often with vulgar or aggressive content), so-called telephone harassment (i.e. where the victim is harassed anonymously and regularly by the victim, often with obscene and threatening telephone calls at any time of the day), but also, more generally, unsolicited e-mails, spam and telephone calls, where repetition can be established.

Because of these characteristics, it can be concluded that this situation has a strong similarity with (cyber)bullying, but the lack of a subordinate-subordinate relationship is a significant difference between the two categories. If we look at the twist of this offence, where the perpetrator contacts the victim by electronic, written or other means on a permanent basis and thereby carries out the harassment, we see that it has a high degree of similarity with the category of *cyberstalking* (a subtype of cyberbullying), but the conceptual elements of this offence can by no means be considered as a sufficient definition of cyberstalking. Accordingly, it must be seen that it is rather difficult to distinguish between this form of harassment and the classic case of cyberstalking, but experience from case law shows that in the Czech Republic this form of harassment [354 § para. (1) point (c)] is usually applied to cases involving cyberstalking.⁵⁷

At the end of our analysis, the following table provides an overview of the correlation between the analysed elements of the Criminal Code and the classic conceptual elements of the category of (cyber)bullying:

Name of the offence	Criminal Code provision	Level of match with (cyber)bullying category ⁵⁸
Breach of confidentiality of forwarded messages	182 § para. (1) points (b)-(c) and para. (2) (b)-(c).	<i>Poor match</i> regularity and continuity is not an element no element of subordination intimidation is not an end, it can only be a result

56 Decision 1333/2013 of the Supreme Court of Justice, Explanatory Memorandum, point 2 [4 Tdo 1333/2013-45 Usnesení NS ze dne 17.12.2013]. The decision is available via the following link: <https://next.codexis.cz/judikatura/JD196188#L1>

57 Vištalová, 2021, p. 24 and p. 27.

58 In this column of the table, we have captured the elements of each of the facts that differ from the classic conceptual elements of the cyberbullying category.

Name of the offence	Criminal Code provision	Level of match with (cyber)bullying category ⁵⁸
Defamation	184. §	<i>Poor match</i> regularity and continuity is not an element no element of subordination intimidation is not an end, it can only be a result
Harassment with sexual intent	186. §	<i>Medium match</i> regularity and continuity is not an element subordination is only a qualifying circumstance
Dangerous threat	353. § para. (1)	<i>Medium match</i> regularity and continuity is not an element no element of subordination
Dangerous harassment	354. § para. (1) points (c) and (e)	<i>Strong match</i> subordination is not a condition

Table 2. Legal elements in the Criminal Code that are similar in content to the category of (cyber)bullying

In conclusion, the Czech criminal legislation contains five legal elements that to a greater or lesser extent correspond to the category of (cyber)bullying. Of the analysed offences, the strongest similarity can be found in the area of harassment, but the offence of harassment with sexual intent, which can be considered a specific type of bullying, should also be highlighted. However, the other three offences analysed (breach of confidentiality of transmitted messages; defamation; threats) show only indirect, weak similarities with the traditional form of (cyber)bullying.

3. Prevention legislation and practice

In terms of prevention, we can report on programmes and procedures in the Czech Republic that are relevant to the topic, especially in relation to bullying in the school environment.

In this respect, it is necessary to briefly refer to the methodological guidance issued by the Ministry of Education, Youth and Sport in 2016 (hereinafter: the Guidance), which deals specifically with the prevention and management

of bullying in educational institutions.⁵⁹ The aim of the Guide is to help educational institutions to understand the phenomenon of bullying, the risks of bullying and how they can prevent and effectively deal with it. The Guidance sets out that educational institutions have a legal obligation to create and maintain a safe environment for pupils, to protect pupils' health and to prevent risky phenomena such as bullying.⁶⁰ In addition, educational institutions should develop *an anti-bullying programme with the primary aim of prevention and the establishment of procedural mechanisms to deal with bullying*. The school management should designate at least one person from among the members of the teaching staff to deal with specific issues of prevention and management of bullying within the educational institution. The designated persons should receive regular training and have the authority to investigate and deal with cases of bullying. As set out in the Guidelines, in order to deal effectively with harassment, the educational institutions concerned should first assess the seriousness of the situation and whether to deal with it internally at the level of the institution or to seek external help (e.g. At the same time, parents always have the right to ask the educational institution or a particular teacher for help in dealing with bullying, and the educational institution has a duty to investigate all suspicions and allegations of bullying. The legal representatives of the parties involved (aggressors, victims and witnesses) should be involved in the investigation and resolution of the problem. If the problem is not satisfactorily resolved by the teachers, the matter should be referred to the head of the school, who has a key role and primary responsibility for preventing and effectively dealing with bullying within the institution. If the school's response is inadequate, it is possible to contact the school's founder or the Czech School Inspectorate (ČŠI).

As far as the so-called *hotlines* (i.e. online counselling and legal aid services) are concerned, it is necessary to highlight the programmes and activities of seven central (public) platforms and NGOs in the fight against harassment:

- a) The 'Minimise harassment' programme (*Minimalizace šikany*)⁶¹
- b) Society against harassment (*Společenství proti šikaně*)⁶²
- c) Internet Counselling Centre (*Internet poradna*)⁶³
- d) Safety line (*Linka bezpečí*)⁶⁴

⁵⁹ The methodology guide is available via the link below: <https://www.msm.cz/file/38988/>

⁶⁰ This obligation is laid down in Article 29 of the Education Act (Act 561/2004).

⁶¹ Available at: <http://www.minimalizacesikany.cz/>

⁶² In this column of the table, we have captured the elements of each of the facts that differ from the classic conceptual elements of the cyberbullying category.

⁶³ Available at: <https://iporadna.cz/>

⁶⁴ Available at: <https://www.linkabezpeci.cz/>

- e) National Internet Safety Centre (*Národní centrum bezpečnějšího internetu*)⁶⁵
- f) E-safety portal (*E-Bezpečí*)⁶⁶
- g) E-Safety portal for teachers (*E-Nebezpečí pro učitele*).⁶⁷

On this topic, it is worth turning our attention for a moment beyond jurisprudence to the work of psychotherapist and therapeutic pedagogue *Michal Kolář*, who has been conducting sociological-based surveys on (cyber)bullying in the Czech Republic for decades. Kolář is also credited with the development of an internationally renowned theory and research model that specifically specialises in the field of school bullying (including cyberbullying). Kolář's theory was the basis for the internationally very positive results of the preventive *anti-bullying programme*⁶⁸, which has been implemented nationwide in the Czech Republic with the support and control of the Ministry of Education. In terms of its effectiveness, Kolář's programme is internationally comparable only with the *Olweus Bullying Prevention Program* (OBPP), which bears the name of *Dan Olweus* from Norway.⁶⁹

4. The issue of service provider liability for offences committed in the online space

It should be noted at the outset that in the Czech Republic there is no specific legislation on social platforms, and thus the Czech legal system does not recognise a public liability regime for the control of content on social media in relation to alleged or actual censorship. At the level of constitutional rules, all forms of censorship, including censorship on the Internet, are prohibited in the Czech Republic, with the proviso that the content and the way in which the information is communicated does not contravene the law.⁷⁰

⁶⁵ Available at: <https://www.ncbi.cz/>

⁶⁶ Available at: <https://www.e-bezpeci.cz/>

⁶⁷ Available at: <http://www.e-nebezpeci.cz/>

⁶⁸ Here is a statistic about the effectiveness of the project: in the pilot schools selected for the programme, the incidence of bullying was reduced by 42.5% in 4 months, while a team of specially trained teachers managed to reduce the number of bullying victims by 50-75%. Later, after the programme was implemented on a larger scale in 50 schools, its effectiveness was confirmed.

⁶⁹ For more on the methodology and experience of Kolář's antibullying programme, see the interview with Kolář: <http://beyondbullies.org/2012/02/program-deals-with-epidemic-in-schools/>

⁷⁰ Cf. Article 17 para. (3) of the Charter.

Currently, social media are not specifically regulated in the Czech legal order, i.e. there is no specific sectoral legislation or other provision concerning social media. At the time of writing, there is no known legislative intention to regulate social media or freedom of expression in this area. Czech law regulates freedom of expression in relation to the Internet and social media only in a tangential manner – This subject is regulated by the *Act on Information Society* (Act No. 480/2004, hereinafter referred to as the ‘Information Law Act’). In view of the year in which this Act was adopted (2004) and its purpose, which was to transpose the rules of the *European Directive on Electronic Commerce*⁷¹ (hereinafter the Directive) into the legislation of the Member States, this Act was not specifically designed to regulate expression and social media on the Internet, but in accordance with the provisions of the Directive, the Czech Act transposes, among others, the rules laid down therein concerning the general liability of hosting providers.

The scope of the Info Act covers the so-called information society services (*služby informační společnosti*). According to the legislation, such services are any information society service which is generally provided for *remuneration*, *at a distance* (i.e. without the simultaneous presence of the parties), *by electronic means* (i.e. the service is sent from its point of origin and received at its destination by means of electronic equipment for processing and storing data, and is sent, transmitted and received entirely by wire, radio, optical or other electromagnetic means) and *at the individual request of the recipient* (i.e. the service is provided by the transmission of data at the individual request).⁷² The Czech case law adds that, in assessing these services, it must be taken into account that:

- a) the service is provided to another person, i.e. it is not for the provider’s own benefit (i.e. services provided, for example, by an employer to its employees for the purpose of their work are excluded); or
- b) that the essence of the service is based on the information transmitted electronically (which excludes, for example, online shops from this scope, because the online interface is merely an intermediary and not the object of the service), and that
- c) it is an individual service for a specific user (which is not the case for example for a radio broadcast).⁷³

71 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. <https://eur-lex.europa.eu/legal-content/HU/TEXT/?uri=celex%3A32000L0031>

72 Zichová, 2019, pp. 21-23.

73 Polčák, 2012, pp. 142-143.

For the reasons set out above, the regulation of this Act approaches the issue under consideration primarily from the perspective of the provision of services on a business basis, rather than from the perspective of the expression of opinion, despite the fact that in certain cases there is an overlap between the two areas.

After an overview of the general rules, let's look at the detailed rules on liability. According to the Information Law Act, the provider⁷⁴ is responsible for the content displayed:

- a) if it was aware, having regard to the subject matter of its activities and the circumstances and nature of the case, that the content of the information stored or the conduct of the user was unlawful; or
- b) if it can be shown that it has knowledge of the unlawful nature of the content of the information stored or of unlawful conduct by the user and has not taken all necessary steps to remove or disable access to such information immediately.⁷⁵

In addition, the service provider is always responsible for the content of the information stored if it directly or indirectly exercises decisive influence over the user's activities.⁷⁶ With these provisions, the legislator transposes the relevant article of the Directive⁷⁷ into Czech law with practically no substantive changes.⁷⁸

In summary, the provider can be held liable for the content it '*transmits*' if the following conditions are met:

- a) the provider's knowledge or knowledge of the infringement; and
- b) the service provider has not removed the infringing content.

As a general rule, the service provider can therefore be held liable if it has not acted after becoming aware of the problem. A special rule, different from this

⁷⁴ It should be noted that the regulation does not distinguish between different types of service providers (e.g. social networking site operator, hosting provider, video-sharing provider). According to the regulation [2 § para. (1) point (a)], a service provider is any person who provides any information society service by electronic means at the individual request of the user, normally against payment. A service is provided by electronic means if it is sent over an electronic communications network and the user accesses it from an electronic storage device.

⁷⁵ Information Law Act 5 § para. (1)

⁷⁶ Information Law Act 5 § para. (2)

⁷⁷ Cf. Czech legislation with Article 14 of the Directive.

⁷⁸ With regard to the legal liability of social media, it should be noted that in addition to the provisions of the Info Law, the provisions of the Civil Code on liability can in principle also be applied.

general rule, is that the provider is liable in all cases where the content is produced directly by him or over which he has a significant influence. This is the case for news portals and online newspapers/magazines, where as publishers they are responsible for the content of the news they publish. This legislation is also in line with the legislation of the Czech Press Law and thus extends its scope to the online space.

Another important provision of the Information Law Act regarding the liability of service providers is that service providers are not obliged to:

- a) monitor the content of the information they transmit or store; and
- b) actively seek out facts and circumstances that suggest illegal content in information.⁷⁹

This means that the service provider has no active content search/content tracking obligations. In this respect, the Czech legislation contains a clear provision which therefore guarantees that active content tracking cannot be imposed on service providers, except in the case of online news portals/newspapers.

The Information Law Act does not contain a public law penalty for failure to remove content that violates the law, so it is a provision without a penalty. Accordingly, in this respect, Czech legislation does not provide for enforcement rules. The concept of infringing content is not defined in detail in the law. Accordingly, it is a broad category covering a wide range of infringements in different branches of law, for which the possible legal consequence or legal disadvantage may take different forms.

It is also necessary to briefly mention that, in addition to the above-mentioned legislation, the possible measures of the service provider in relation to the expression of opinions and the possibilities of taking action against the user are also reflected in the general terms and conditions of each service provider (hereinafter: GTC). These are bilateral private agreements between the service provider and the user. The general approach of such GTCs is that service providers reserve the right to remove content that is in breach of the law.

In conclusion, two trends have emerged in the Czech Republic in recent years with regard to the obligation for Community platforms to intervene. The first advocates accountability and responsibility of social media, arguing that service providers are able to control the source of the threat, while at the same time being able to easily avert the threat of infringement to the extent of their

⁷⁹ Information Law Act 6 §.

capabilities.⁸⁰ The other approach is that service providers cannot be obliged to actively monitor content under the regime of the Information Law Act.⁸¹

Following the overview of liability issues, it is important to briefly point out that Czech law does not recognise the criminal measure of making electronic data inaccessible in Hungarian terminology, and at the same time Czech law does not recognise a category of criminal offences equivalent in content to the making of electronic data inaccessible in Hungarian terminology, so that such criminal measures cannot be applied to offences committed in online space, including cyberbullying.⁸² The penalties for the offences described above are, as a general rule, imprisonment and, in some cases, disqualification from practising. It should also be noted that Czech law does not contain any specific provisions for the effective prosecution of hate speech and cyberbullying offences committed online (e.g. the possibility to obtain legal assistance and to request the authorities).

Summary

Although Czech legislation does not recognise the category of hate speech, the criminal legislation does contain a number of elements that correspond to this category or have a close substantive connection with it. The Criminal Code accordingly criminalises and punishes certain forms of hate speech. After analysing the relevant criminal law provisions, it can also be concluded that hate speech offences can be committed both offline and online, and that the offender committing an offence online is considered a qualified offence. In this context, it is also important to underline that Czech case-law already classifies as hate speech the expression of an opinion or value judgement that incites hatred against a specific group of persons in the form of a comment on a post on a social media platform.

Similar to the category of hate speech, Czech law does not recognise the categories of *bullying* and *cyberbullying*, so neither the Criminal Code nor any other legislation establishes them as separate elements of crime, while the Criminal Code does, however, include several elements that contain elements of the conceptual elements of these categories. The Penal Code sets out five legal elements

⁸⁰ Telec, 2015, p. 20.

⁸¹ For more on this, see Maisner, 2015.

⁸² For more information on the sanction system of the Czech Penal Code, see the Penal Code 36-104 §.

which are identical to the category of (cyber)bullying. After analysing these elements, it is concluded that the strongest similarity with cyberbullying can be found in the case of *harassment*. In addition to this offence, the offence of *harassment with sexual intent*, which can be considered as a specific type of bullying, should also be highlighted. However, the other three offences analysed (breach of confidentiality of transmitted messages; defamation; threats) show only an indirect, weak correspondence with the category of (cyber)bullying.

As regards the issue of prevention, there are programmes, procedures and professional documents, particularly in relation to bullying in the school environment, which are both preventive and effective in dealing with bullying situations.

In the Czech legal order, there is no specific legislation on social platforms, and therefore no legislation on content control in social media. With regard to the issue of service provider liability, Czech law generally provides that a service provider can be held liable for the content it transmits if it knew or became aware of the infringement and did not remove the infringing content. In short, the service provider can therefore be held liable if it failed to act after becoming aware of the infringement. However, the service provider is liable in all cases where it directly produced the content or had a significant influence on the content itself. A further important rule is that service providers are not under an active obligation to search for and monitor the content of the information they store and transmit.

Bibliography

- Bartoň, M., Hejč, D. (2021) 'Čl. 17 [Svoboda projevu a právo na informace]' in Husseini, F., Bartoň, M., Kokeš, M., Kopa, M. (eds.) *Listina základních práv a svobod*. 1st edition, Praha: C.H. Beck.
- Fremr, R. (2015) 'Trestné činy proti lidské důstojnosti v sexuální oblasti' in Drašík, A. et al. (eds.) *Trestní zákoník: komentář*. 1st edition, Praha: Wolters Kluwer.
- Herczeg, J. (2004) *Meze svobody projevu*. Praha: Orac.
- Holas, J. (2012) *Trestné činy proti lidské důstojnosti v sexuální oblasti*. Olomouc: Univerzita Palackého v Olomouci.
- Maisner, M. (2015) 'Snaha o zakázané těžení ze zdánlivé absence výslovné legislativní úpravy a nebezpečná situace pro poskytovatele služeb informační společnosti', *Bulletin advokacie* [online] <http://www.bulletin-advokacie.cz/snaha-o-zakazane-tezeni-ze-zdanlive-absence-vyslovne-legislativni-upravy>
- Nováková, H. (2010) *Trestné činy narušující soužití lidí z hlediska nové právní úpravy*. Brno: Právnická fakulta Masarykovy univerzity, Katedra trestního práva.
- Parti, K. (2016) 'A megfélemlítés (bullying) szabályozása Magyarországon és külföldön', *In Medias Res*, 5(1), pp. 114-146.
- Polčák, R. (2012) *Internet a proměny práva*. Praha: Auditorium s.r.o.
- Šámal, P. (2012) *Trestní zákoník: komentář*. 2nd edition, Praha: C.H. Beck.
- Ščerba, F. (2009) 'Trestné činy proti důstojnosti v sexuální oblasti' in Jelínek, J. (ed.) *Trestní právo hmotné*. 1st edition, Praha: Leges.
- Strakoš, J. (2021) 'Šíření nenávisti na internetu a jeho trestní postihy (poznatky k limitům českého přestupkového práva a úvahy nad nimi)', *Správní právo*, 54(1) [online] <https://www.mvcr.cz/clanek/spravni-pravo-cislo-1-2021.aspx>
- Telec, I. (2015) 'Zakázané těžení a nebezpečná situace na elektronických úložištích dat', *Bulletin advokacie*, 2015/1-2, pp. 19-29. [online] http://www.bulletin-advokacie.cz/assets/zdroje/casopis/2015/BA_1-2_2015_web.pdf
- Vištalová, A. (2021) *Trestněprávní aspekty kyberšikany*. Praha: Právnická fakulta Univerzita Karlova, Katedra trestního práva.
- Zichová, T. (2019) *Odpovědnost poskytovatelů služeb informační společnosti za cizí obsah*. Brno: Právnická fakulta Masarykovy univerzity.

VIII. HATE SPEECH AND CYBERBULLYING IN THE POLISH LEGAL REGULATION

MÁRTA SAROLTA DEÁK

1. Introduction

The issue of cyberbullying has been a recent topic in Poland. Many attempts were made to tackle this problem. The approach may vary as many try to find a solution such as the field of education, psychology or the legislation. This article aims to introduce the reader to the regulatory issues of hate speech and cyberbullying in Poland.

I would like to thank Márta Benyusz for her collaboration to the chapter.

2. Regulatory Issues on Hate Speech

2.1. Freedom of Expression and its Limitations

Freedom of speech and expression is an essential and broadly recognized element of the Polish legal system.¹ The inherent and inalienable dignity of each and every human being is one of the foundations of the Polish legal system. Furthermore, it is also the source of the legislation related to freedom of speech and expression as well as its limitations (e.g. hate speech). The Polish Constitution²

¹ Bojanowski, p. 176.

² Konstytucja Rzeczypospolitej Polski z dnia 2 kwietnia 1997 r. <https://www.sejm.gov.pl/prawo/konst/angielski/kon1.htm>

(Konstytucja Rzeczypospolitej Polski, hereinafter referred to as the Constitution) declares that „the inherent and inalienable dignity of the person shall constitute a source of freedoms and rights of persons and citizens. It shall be inviolable. The respect and protection thereof shall be the obligation of public authorities” (Article 30). This article is the origin of many important principles such as

- freedom of the press (wolność prasy i środków społecznego przekazu – Article 14),
- freedom of religion and conscience (wolność sumienia i wyznania – Article 53) and
- freedom of speech (wolność słowa – Article 54).

Freedom of speech regulated by Article 54 includes freedom of expression and the right to information (wolność wypowiedzi i informacji) and prohibition of censorship. According to the Polish Constitutional Court (Trybunał Konstytucyjny, hereinafter referred to as TK), freedom of speech as established by the Constitution „covers an individual’s activity as its whole, is an instrument of the dignified expression of an individual autonomy, creating the possibility for the complete development of the individual’s personality in the surrounding cultural and civilisational environment”.³

Pursuant to Article 31 of the Constitution, limitations upon the exercise of constitutional freedoms and rights – including freedom of expression – „may be imposed only by statute, and only when necessary in a democratic state for the protection of its security or public order, or to protect the natural environment, health or public morals, or the freedoms and rights of other persons. Such limitations shall not violate the essence of freedoms and rights.”

Statutory regulations concerning freedom of speech are incorporated in the Civil Code (Kodeks Cywilny), the Criminal Code (Kodeks Karny), the Law on the Protection of State Secrets (Ustawa o ochronie tajemnicy państwowej), the Copyright Act (Prawo autorskie),⁴ the Press Act (Prawo prasowe)⁵ and the Radio and Television Broadcasting Act (Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji).⁶

3 TK: z 12.05.2008 r., SK 43/05, OTK-A 2008/4, poz. 57; z 14.12.2011 r., SK 42/09, OTK-A 2011/10, poz. Decisions No.

4 Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych. <http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19940240083/U/D19940083Lj.pdf>.

5 Ustawa z dnia 26 stycznia 1984 r.

Prawo prasowe <http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19840050024/U/D19840024Lj.pdf>

6 Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji <http://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20170001414/U/D20171414Lj.pdf>

The so-called guardians of freedom of speech and expression are the TK and the courts, as well as the National Broadcasting Council (Krajowa Rada Radiofonii i Telewizji – hereinafter referred to as KRRiT)⁷ and the National Media Council (Rada Mediów Narodowych – hereinafter referred to as RMN). Pursuant to Article 213 of the Constitution, the KRRiT is responsible for safeguarding freedom of expression and the right to information. Additionally, protecting the public interest in radio and television broadcasting also falls within the scope of the KRRiT. The scope and the functioning of the KRRiT is regulated by Chapter 2 of the Radio and Television Broadcasting Act. There are three main functions:

- to ensure freedom of expression and independence of broadcasters,
- to protect the interests of viewers and listeners and
- to maintain the transparency and pluralism of the radio and television market.

The RMN was established in 2016⁸ with the capacity to appoint and dismiss members of the governing bodies of public service media (radio and television) and of the Polish Press Agency (Polska Agencja Prasowa)⁹. The RMN also performs other tasks specified by law. When selecting its members, the RMN aims to select individuals capable to guarantee compliance with the law and media and editorial independence.

2.2. Hate Speech Regulations

Hate speech is not expressly defined by Polish legislation. The legal literature refers to the 1997 Recommendation of the Committee of Ministers of the Council of Europe¹⁰ which characterizes hate speech as „all forms of expression which spread, incite, promote or justify racial hatred, xenophobia, anti-Semitism or other forms of hatred based on intolerance, including: intolerance expressed by aggressive nationalism and ethnocentrism, discrimination and hostility against minorities, migrants and people of immigrant origin.”

Despite the lack of a precise legal definition the Polish legal system protects freedom of expression as evidenced by the aforementioned constitutional norms and the resulting statutory principles. However, also interferes with it

⁷ <http://www.krrit.gov.pl/>

⁸ Ustawa z dnia 22 czerwca 2016 r. o Radzie Mediów Narodowych <http://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20160000929>

⁹ <https://www.pap.pl/>

¹⁰ Recommendation No R (97) 20 of the Committee of Ministers of the Council of Europe on „Hate Speech”. https://search.coe.int/cm/Pages/result_details.aspx?ObjectID=0900001680505d5b

via the provisions criminalising expressions of hate, thus subsequently making the prohibition of hate speech a limitation on freedom of speech.¹¹ According to Article 256 of the Criminal Code, „anyone who publicly promotes a nazist, communist, fascist or other totalitarian system of state, or incites hatred based on national, ethnic, racial or religious differences or for not being religious, is liable to imprisonment for up to three years. The same punishment shall be imposed on anyone who distributes, produces, records, or brings, acquires, stores, possesses, presents, carries or sends any print, recording or other object containing the content specified previously, or bearing fascist, communist or other totalitarian symbolism. No offence is committed by anyone who commits such an act in the context of artistic, educational, collector or scientific activity.” Further limitations are also specified by the Criminal Code in Articles 117-119, 127-130, 133, 134-135, 137, 140, 148-150, 189-189a, 190a, 194-204, 222-224a, 249-251, 255-258 and 343. These limitations typically include hate crimes, crimes against the State, crimes against life or health and incitement to do so, crimes against liberty, crimes against freedom of conscience and religion, crimes against sexual autonomy and integrity and incitement to do so, crimes against State and local government bodies, offences against the fairness of elections, crimes against public order, disobeying military orders. Pursuant to Article 18 of the Radio and Television Broadcasting Act, radio and television programmes may not promote unlawful conduct or attitude contrary to the order of the Polish state, morality and social good. In particular, they may not contain incitement to hatred or violence, discriminatory content in connection with gender, race, ethnicity or social status, genetic characteristics, language, religious, political or other convictions, nationality or minority status, property, birth, disability, age or sexual orientation or incitement to commit terrorist acts.

Based on the Polish legislation, there are three distinctive types of hate speech worth mentioning. These are as follows:

- offline hate speech concluded by politicians or public personalities,
- other miscellaneous types of offline hate speech, and
- online hate speech.

A resolution of the Lower Chamber of the Polish Parliament (Sejm) of 17 July 1988 on the ethical principles of parliamentary operations establishes that Members of Parliament must refrain from any conduct which might damage the reputation of the Parliament and must respect the human dignity of others in all circumstances. The Ethics Committee of the Sejm may issue a warning or

¹¹ Bojanowski, p. 178.

reprimand to a Member who violates ethical principles. The Ethics Committee of the Upper Chamber (Senate) has similar scope, i.e. can warn and reprimand a senator who behaves in a manner ‘unbecoming to a senator’. Both the members of the Lower the Upper Chamber have immunity. This means that even if the conduct in question falls within the scope of criminal law, the prosecution is conditional on his or her voluntary waiver of immunity or on the Parliament’s depriving him or her of it.

The Polish state currently does not monitor online hate speech actively, but reacts on a case-by-case basis on the basis of indictments. The Warsaw District Court’s decision of 12 June 2019 is a prime example of judicial action against online hate speech in the context of incitement to violence. According to the decision, ‘M.L.’ incited hatred against a group of people on the basis of religion and nationality in a post on Twitter, calling for violence against them and for the killing of people to harm them. The legal basis for the decision was Article 126a of the Polish Criminal Code (promotion of dictatorship, public provocation to commit an offence against peace), together with Article 255 § 2 (provocation to commit an offence) and Article 256 § 1 (incitement against a group of people). None of the facts is specifically tailored to online hate speech, but all include incitement as prohibited conduct.

On 26 February 2014, the Polish Prosecutor General (Prokurator Generalny) issued guidelines on the conduct to be followed in hate crime proceedings in order to unify and harmonise the application of the law in hate crime cases. According to point 14 of the Guidelines, all hate crime cases in Poland must be treated as a priority, which in practice means that prior to the indictment, during the investigation phase, the case and its circumstances must be reported to the prosecutor in charge and that he/she must be kept informed of the progress throughout the proceedings. On the basis of the information received, the senior prosecutor will assess the case and decide whether it is necessary to formally bring it under his supervision. All cases involving hate crime require close internal supervision by the prosecutor. Cases that are not ultimately prosecuted are subject to periodic monitoring by the superior prosecutor’s office to ensure that the proceedings are conducted fairly and that the decision on the merits is valid. Specific institutional reforms have been adopted in order to increase the efficiency of procedures, including in particular the effective protection of victims’ rights. A special unit has been created in each district prosecutor’s office to investigate such crimes. Each unit must have at least two prosecutors in charge who are assisted by advisers. The measures have led to the creation of a team of prosecutors in Poland who specialise in hate crimes.

Poland regularly provides data and statistics¹² on hate crimes (including hate speech) to the Office for Democratic Institutions and Human Rights (hereinafter ODIHR).¹³ Although hate speech itself is not explicitly part of the definition used by the Organisation for Security and Co-operation in Europe and thus by ODIHR, the statistics themselves include conducts of hate speech nature. According to these statistics, one could deduct that the ratio of successful convictions in hate crimes cases is on a rise, which means that the courts are becoming more and more aware and sensitive to the issue.

Year	Hate crimes reported to the police	Number of convictions	Number of sentences
2023	893	386	296
2022	1180	440	312
2021	826	466	339
2020	826	374	266
2019	972	432	597
2018	1117	397	315
2017	886	320	260
2016	874	281	236

Table 3. The ratio of successful convictions in hate crimes cases is on a rise

3. The Regulation of Cyberbullying

3.1. Regulatory Framework

Cyberbullying (cyberprzemoc) is a form of violence that involves the use of electronic devices, usually a phone or computer. The aim is always to cause harm to another person. Like traditional violence, cyberbullying is a systematic, premeditated action against weaker persons who cannot defend themselves.¹⁴ Cyberbullying is difficult to regulate because the definition of key concepts and the clear distinction between them are unclear and can cause difficulties for legislators. This is still a grey area in legal science, as there are several subjective elements to the issue, which makes it difficult to objectively assess individual cases. Since the legal literature does not provide a more precise definition,

¹² <https://hatecrime.osce.org/poland>

¹³ <https://hatecrime.osce.org/>

¹⁴ NASK ACADEMY, p.8.

other concerned fields (eg. social norms, education or workplace regulations) can assist law enforcement to interpret cyberbullying.

In Poland, criminal prosecution of cyberbullying was made possible by an amendment to the Polish Criminal Code¹⁵ which entered into force on 6 June 2011 and criminalises certain forms of cyberbullying. According to the explanatory memorandum to the amendment, the aim was to criminalise persistent harassment.¹⁶ Before 2011, harassment was not a criminal offence under the Polish Criminal Code. The most similar conduct that was regulated by the legislator was malicious annoyance as defined by the Code of Offences of 1971¹⁷ (Kodeks wykroczeń). Malicious annoyance was committed when the perpetrator maliciously misled or otherwise disturbed another person in bad faith with the purpose of annoying him/her.¹⁸

In addition to harassment, the grounds for prosecution of cyberbullying may also be based on the following articles of the Code of Offences:

- Art. 190 (groźba karalna – criminal offence),
- Art. 212 (zniesławienie – defamation),
- Art. 216 (zniewaga – insult),
- Art. 267 (bezprawne uzyskanie informacji – unlawful acquisition of information),
- Art. 268. (utrudnianie zapoznania się z informacją – making it difficult to obtain information),
- Art. 268a (niszczenie danych informatycznych – destruction of computer data),
- Art. 107. (złośliwe niepokojenie drugiego człowieka – malicious interference with another person),
- Art. 141 (nieobyczajne ogłoszenie, napis, rysunek – indecent advertising, inscription, drawing).¹⁹

15 Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (t.j. Dz. U. z 2022 r. poz. 1138). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19970880553>

16 Kania Marcin: Stalking a windykacja, ABC.

17 Ustawa z dnia 20 maja 1971 r. Kodeks wykroczeń (t.j. Dz. U. z 2021 r. poz. 2008 z późn. zm.). <https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=wdu19710120114>

18 Ustawa z dnia 2 maja 1971 r. Art. 107. Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 3000 złotych albo karze nagany.

19 Las, Katarzyna: Odpowiedzialność karna za zjawisko cyberprzemocy w świetle prawodawstwa polskiego. Rocznik Bezpieczeństwa Międzynarodowego, 14(1), 256-277. <https://doi.org/10.34862/rbm.2020.1.15>

On the civil law side of the issue, cyberbullying concerns the personality rights. The Polish Civil Code touches on this subject in Articles 23 (dobra osobiste człowieka – rights of the personality) and 24 (ochrona dóbr osobistych – protection of the rights of the personality).

Henceforth, the provisions of Article 190a (uporczywe nękanie, kradzież tożsamości – persistent harassment and identity theft) of the Criminal Code will be interpreted along with the relevant case law.

The crime of harassment may be committed by four different types of conduct. Pursuant to Article 190a §1 of the Criminal Code, whoever, by persistently harassing (uporczywe nękanie) someone or a person close to someone, creates a feeling of danger (zagrożenia), humiliation (poniżenia) or torture (udręczenia) in that person or causes substantial invasion of privacy, is punishable by imprisonment for a term of between six months and eight years.²⁰ According to the interpretation of the law, harassment is considered psychological violence,²¹ the perpetrator must create a legitimate sense of danger, humiliation or (internal) torture in the victim or seriously violate his/her personal sphere in order to this legal offence to be committed.

Originally, Article 190a of the Criminal Code in 2011 established only two types of conduct of harassment. In March 2020 the scope of harassment was expanded by establishing that it may be committed by causing a feeling of humiliation or torment.²² According to the provisions of § 2, anyone who, by impersonating another person, using that person's image, other personal data or any other data by means of which that person can be publicly identified, with the purpose of causing material or personal damage, shall also be liable to the penalty laid down in § 1. These provisions approach the offence of harassment from a personality law perspective and constitute another offence, identity theft. Article 3 provides for a qualified case of the offence of harassment: if the victim commits suicide as a result of an act as defined in Article 1 or 2, the offender is punishable with imprisonment for a term of 2 to 12 years. Article 190a(4) provides that proceedings may be brought on the private initiative of the victim in respect of an act as defined in § 1 or § 2.²³

20 Kodeks Karny Art. 190a § 1. Kto przez uporczywe nękanie innej osoby lub osoby jej najbliższej wzbudza u niej uzasadnione okolicznościami poczucie zagrożenia, poniżenia lub udręczenia lub istotnie narusza jej prywatność, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.

21 Ćmiel, Sylwia: Cyberbullying legislation In Poland And Selected EU Countries.

22 Budyn-Kulik, Magdalena: Nowe znamiona nękania z Art. 190a § 1 Kodeksu karnego.

23 Kodeks Karny Art. 190a § 4. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

The legal object of the offence of harassment as defined in Article 190a § 1 of the Penal Code is the psychological freedom or well-being of the person, and also, human life as regulated by § 3. The offence may be committed against another person or the person closest to him/her (relative). Harassment may be committed directly or indirectly. The legislation reflects on this approach as the distinction is made between the different targets of the act. The concept of 'relative' is set out in Article 115(11) of the Criminal Code in the form of a taxonomy. According to this definition, the spouse, ancestors, descendants, other relatives in the same or direct line, adopted child and his/her spouse, and life partner.²⁴

The offence may be committed by persistent harassment. The term harassment is not clearly defined by law. The persistent nature of the conduct refers to an act that is continuous over a long period of time. There is an objective and a subjective condition for persistent harassment. Objectively, the act must be a repeatable. Thus, an act that cannot be committed more than once may not fall within the scope of harassment. Subjectively, there must be a determination and a specific effort on the part of the perpetrator to carry out the harassment.²⁵ It also follows that the negligent form of the offence is conceptually excluded, only intentional commission is possible.

Harassment is an outcome crime. The four different outcomes are as follows:

- the creation of a sense of threat,
- or humiliation,
- or distress in the target, or
- a serious violation of the victim's privacy.

As these are alternatives to each other, the legal offence of harassment can be exhausted by any of these outcomes.

The sense of threat must be justified by the circumstances. There must be a causal connection between the offender's actions and the victim's state of mind. This is an objective scale which is not clearly defined by the legislation and remains for the judiciary to interpret. Justified sense of threat was found in a case when a minor was distressed and made to flee by the defendant.²⁶ In another case the defendant provoked a violent emotional reaction from the victim by his harassing messages.²⁷ In a third case the court found that the height-

²⁴ Kodeks Karny Art. 115 § 11. osobą najbliższą jest małżonek, wstępny, zstępny, rodzeństwo, powinowaty w tej samej linii lub stopniu, osoba pozostająca w stosunku przysposobienia oraz jej małżonek, a także osoba pozostająca we wspólnym pożyciu.

²⁵ Janczukowicz.

²⁶ Wyrok SO w Gliwicach z 16.10.2018 r., VI Ka 893/18, LEX nr 2638002.

²⁷ Wyrok SO w Gliwicach z 27.08.2018 r., V Ka 255/18, LEX nr 2553186.

ened emotional state and impulsive behaviour of the accused could justifiably cause fear in the victim.²⁸ According to case law, in the case of the statutory offence of harassment, the feeling of being threatened is a continuous, gradual reduction in the victim's sense of security as a result of repeated acts by the perpetrator.²⁹ Accordingly, where there is no repetitive nature, it can no longer be established that the perpetrator's conduct creates a continuing sense of threat.

The feeling of humiliation is mentioned in several places in the Criminal Code, yet it is difficult to define its exact meaning, as the legislator uses the term in different contexts.³⁰ For example, Article 212 of the Criminal Code describes humiliation as a conduct likely to degrade the victim in the eyes of the public or to expose the victim to a loss of confidence in his or her profession. In the absence of a more precise wording, this is the origo for the interpretation of Article 190a of the Criminal Code.

The concept of torture is also lacks an exact definiton in the legislation. Article 190a of the Criminal Code refers to the term *udręczenie*, but the concept of special torture (*szczególne udręczenie*) is also applied several times and is widely discussed in the legal literature. The Polish dictionary defines this term as physical or mental suffering caused to another person.³¹ On this basis, it can be concluded that – for the purposes of this provision – the torture inflicted may be both physical and psychological in nature.

With regard to the real and significant invasion of privacy, the Supreme Court has stated in one of its most important judgments that the use of the term 'significant' in the text of the norm is not in vain, since it is the measure of the degree of invasion of privacy, which allows to determine the intensity of the act.³² In the same judgment, the court also stated that the violation of privacy occurs at the moment of the unauthorised intrusion into the personal sphere of the victim. Thus, for example, if the offender secretly makes recordings of the victim, regardless of the quantity and the subsequent fate of the recordings, the violation of privacy is already established by the content of the recordings at the moment of making the first recording.

By criminalising identity theft, the legislative aim is to protect people's rights as individuals, such as the protection of personal image, the right to the protection of personal data and the right to the protection of other data that facilitate identification. Unlike persistent harassment, identity theft does not require the

28 Wyrok SO w Gliwicach z 13.03.2018 r., VI Ka 155/18, LEX nr 2561794.

29 Wyrok SO w Elblągu z 22.11.2018 r., VI Ka 476/18, LEX no 2614930.

30 Budyn-Kulik.

31 <https://sjp.pwn.pl/szukaj/Udr%C4%99czenie.html>

32 Wyrok SN z 12.01.2016 r., IV KK 196/15, LEX no 1976249.

repeated commission of the same act, but the offence may be committed only once by the conduct defined by law. It is also an outcome crime, where the result is the harm caused to another person by the offender impersonating another person by unlawfully using personal identification marks. The law defines such identification marks as a photograph, personal data, and any other data that can be used to identify a person. Only the data of a real, natural person can be used, as the data of a fictitious person are not considered personal data.³³ The subjective aspect of the offence involves the intention of the perpetrator to cause harm to others, so that here too negligence is excluded and there must be a direct intention to commit the offence.

Article 190a(3) criminalises the more serious offences of persistent harassment and identity theft where the victim commits suicide as a result of the offender's behaviour. This is also a substantive offence, resulting in an attempt on the victim's life. Attempted suicide is sufficient to establish the offence.³⁴

3.2. Legal Practice

The Polish judicial practice has provided a lot of guidance as to what exactly constitutes harassment or even cyberbullying. The most common form of harassment are stalking and direct physical contact with the target.³⁵ This can also include unsolicited and repeated contact with the target via Internet sites, which is understood as cyberbullying by the everyday vernacular. Another typical form of harassment occurs in writing, i.e. the repeated sending of letters, e-mails or SMS messages. In this context, it should be emphasized that several court judgments³⁶ have shown that the assessment of the content of electronic forms of contact, such as e-mail or SMS messages, is no different from the assessment of liability for traditional 'offline' harassment. The content of the message, the language used and the assessment of the circumstances are much more important in determining the facts of the case than the way in which the message reaches the victim.

In the case of harassment by messages on social media, the judicial practice emphasized the importance of the frequency of messages sent when finding

33 Mozgawa, Marek: Kodeks karny. Komentarz, WKP 2021. <https://sip.lex.pl/#/publication/151396710/kodeks-karny-komentarz>

34 Mozgawa.

35 Janczukowicz.

36 Wyrok SO w Poznaniu z 28.08.2018 r., IV Ka 697/18, LEX nr 2574554., Wyrok SO w Warszawie z 7.09.2018 r., VI Ka 1612/17, LEX nr 2568459., Wyrok SO w Sieradzu z 18.04.2018 r., II Ka 59/18, LEX nr 2485253., Wyrok SO w Sieradzu z 23.10.2019 r., II Ka 226/19, LEX nr 2760463.

harassment. In one case, a primary school teacher regularly sent messages to his 14-year-old student on social media sites, regardless of the time of day, which seriously violated the victim's privacy.³⁷ An essential element for understanding the current regulatory environment is the fact that in the case in question the court did not take the victim's age into consideration. The statutory definition does not distinguish between cyberbullying offences committed against minors and those committed against adults.

Photographing or making videos of the victim may also constitute harassment if it is likely to violate his/her privacy. Exempt from this clause is when the recording in question occurs in a public place which is accessible to all or if the perpetrator documents an otherwise neutral activity.³⁸ Two judgments of the Polish Supreme Court are relevant in this context.³⁹ In one case, the court held that the invasion of privacy occurs at the moment of recording and that the character of the act is not determined by the nature of the material produced, but by the mere fact of interference, i.e. the unauthorised intrusion into the private sphere. The Court found that it is difficult to find a situation in which persistent harassment is not accompanied by a significant violation of privacy. In this judgment, the court also referred to the 'substantial harm' test, which has been discussed above. Harassment by means of photographs or video recordings was also found to exist, for example, where the perpetrator regularly photographed and videotaped the victims on a building plot owned by their daughter over a period of two months and made offensive comments about them.⁴⁰

3.3. Abuse at Work or in an Educational Institution

The abusive nature of cyberbullying may be of concern if it could jeopardise the academic or professional progress of the target. For this reason, particular attention should be paid to bullying at work or school, as these acts can also typically cause feelings of fear, humiliation or embarrassment for the perpetrator.⁴¹

The Labour Code⁴² (Kodeks pracy) lists establishment and enforcement of rules of social coexistence in the workplace in Article 94 (10) among the

37 Wyrok SO w Toruniu z 25.05.2017 r., IX Ka 189/17, LEX nr 2362424.

38 Janczukowicz.

39 Wyrok SN z 29.03.2017 r., IV KK 413/16, OSNKW 2017, nr 8, poz. 44., Wyrok SN z 12.01.2016 r., IV KK 196/15, LEX nr 1976249.

40 Wyrok SO w Toruniu z 17.08.2017 r., IX Ka 839/16, LEX nr 2549861.

41 Marciniak, Jarosław: Praktyka sądowa dotycząca zjawiska mobbingu, ABC. <https://sip.lex.pl/#/publication/469911290?keyword=Poni%C5%BCenia>

42 Ustawa z dnia 26 czerwca 1974 r. Kodeks pracy (t.j. Dz. U. z 2020 r. poz. 1320 z późn. zm.). [https://sip.lex.pl/#/act/16789274?unitId=art\(94\)&cm=DOCUMENT](https://sip.lex.pl/#/act/16789274?unitId=art(94)&cm=DOCUMENT)

obligations of the employer. Article 943 is even more specific, containing provisions on the phenomenon of the so-called mobbing. The law defines mobbing as any act or conduct directed at or against an employee which results in or is intended to result in persistent and prolonged harassment or intimidation of the employee, which leads to the reduction of the employee's professional self-esteem, the belittling or ridicule of the employee, isolation or exclusion from the group of co-workers.⁴³ The law establishes the employer's duty to take action against mobbing and also provides that an employee who suffers harm as a result of mobbing may claim compensation. Furthermore if an employee terminates his/her employment contract as a result of bullying, he/she must do so in writing, stating the reason for the termination. This practice may reduce the latency of the bullying. However, statistics show that mobbing cases are unlikely to succeed, as courts are very cautious about determining whether or not mobbing has occurred.⁴⁴ Just like with all similar cases, there is a high latency rate.

In relation to school bullying and peer bullying, it is worth pointing out that under the provisions of the Criminal Code, peer bullying of children under the age of 18 is not punishable. Therefore the criminalisation of minor-on-minor cyberbullying of a controversial field of law.

The problem of cyberbullying in educational institutions was researched by the Polish State Audit Office in 2017.⁴⁵ The results showed that the Ministry of Education, the schools and the police are not really aware of the grave risks of cyberbullying for children and young people. The study found that amongst those surveyed, 40% of the children, 35% of the parents and 45% of the teachers have been affected by some form of cyberbullying. Despite this, schools are yet to develop guidelines or policies to help combat the phenomenon. The research has identified the high latency in this area and the risk of harm, not only to the individual but to a whole group. The study also found that, although the phenomenon of contemporary abuse is unfortunately not a recent phenomenon, the technical developments provide a wider range of tools that may be used to cause harm. Furthermore, the study highlighted the importance of prevention and the key role of parents in particular. Nevertheless, parents cannot be left alone with this problem to tackle and need the support of schools and the

43 Penal Code Art. 943 §1. Mobbing oznacza działania lub zachowania dotyczące pracownika lub skierowane przeciwko pracownikowi, polegające na uporczywym i długotrwałym nękaniu lub zastraszaniu pracownika, wywołujące u niego zaniżoną ocenę przydatności zawodowej, powodujące lub mające na celu poniżenie lub ośmieszenie pracownika, izolowanie go lub wyeliminowanie z zespołu współpracowników.

44 Marciniak.

45 <https://www.nik.gov.pl/plik/id,15249,vp,17730.pdf>

police. In addition to the many negative findings, the research also noted positively the sensitive response of school staff in cases where an incident came to their attention.

3.4. The Connection Between Cyberbullying and Hate Speech

When assessing the Polish legal system, it is particularly difficult to make the connection between cyberbullying and hate speech as neither separate legal offences. In distinguishing between hate speech offences and cyberbullying cases, the repetitive nature of the latter is the deciding factor. In the case of hate speech regulations the continuous or repeated nature of the act is not a key concept of the conduct.⁴⁶ Hate speech involves verbal aggression, whereas cyberbullying is much more nuanced, as it can be committed physically, verbally and also by passive behaviour.⁴⁷ What they have in common is aggression and the targeting of a specific person or group.⁴⁸ It should be noted that Polish criminal law does not include discrimination on the grounds of sexual orientation and disability in the definition of hate speech under Article 257 of the Criminal Code, which is the article closest to the concept of hate speech.⁴⁹

4. Preventive Legislation and Practice

As there are no specific legal provisions to prevent cyberbullying, one needs to refer to other areas of expertise such as pedagogy and psychology. The research institute NASK (Naukowa i Akademicka Sieć Komputerowa)⁵⁰ supervised by the Polish Prime Minister's Office together with the National Education Network (Ogólnopolska Sieć Edukacyjna)⁵¹ has produced a manual⁵² on the prevention of cyberbullying in schools, primarily addressed to teachers. In the following section, the content of the handbook is analysed.

46 Bedrosova, Marie – Machackova, Hana – Šerek, Jan – Smahel, David – Blaya, Catherine: The relation between the cyberhate and cyberbullying experiences of adolescents in the Czech Republic, Poland, and Slovakia, *Computers in Human Behavior*, Volume 126, 2022.

47 Wiczorkowski, Jędrzej – Suwińska, Aleksandra: *Mowa nienawiści w mediach społecznościowych*.

48 Bedrosova – Machackova – Šerek – Smahel – Blaya.

49 Wiczorkowski – Suwińska.

50 <https://www.nask.pl/>

51 <https://ose.gov.pl/>

52 <https://it-szkola.edu.pl/publikacje,plik,71>

Firstly, the material begins with a definition of cyberbullying. In this approach, cyberbullying takes place primarily on social media, online communication spaces and online games. Cyberbullying is often a form of peer aggression. The manual cites a case from 2006 when a 14-year-old girl in Gdansk was stripped naked and sexually abused by her peers in the classroom at a time when the teacher was not present. A video of the incident was also recorded and the girl was constantly threatened by uploading it on the internet. The girl eventually committed suicide. In the wake of the incident, the Ministry of National Education (Ministerstwo Edukacji Narodowej) launched the Zero Tolerance for Bullying Programme (Zero tolerancji dla przemocy w szkole).⁵³ The programme was run by the government and was implemented by state departments, municipalities, police, civil guards, NGOs, churches, schools and educational institutions, as well as training institutions for teachers. The programme has received a lot of criticism for its focus on retaliation rather than prevention.

The handbook compares cyberbullying with ‘traditional’ bullying of the peers. Without taking away from the seriousness of ‘traditional’ bullying of the peers, the handbook argues that tackling cyberbullying is a much more difficult task. In this regard, five characteristics of cyberbullying are highlighted: (i) its ability to reach large audiences (ii) in a very short time, (iii) the anonymity of the perpetrator, (iv) the borderless nature of the act, and (v) the complete lack of adult control. Assessing the effects of cyberbullying, the emotional difficulties of victim are emphasized, especially loneliness, humiliation, helplessness, fear, sadness and shame. Prolonged abuse affects the victim’s way of thinking about themselves and the world around them. They may have serious difficulties in later life with relationships, self-esteem, education and psychological or physical health problems are also frequent. Suicidal thoughts and attempts are also common.

The parents’ tools to prevent and avoid cyberbullying are also outlined. The importance of continuous communication and dialogue with the child is highlighted, including discussions on the rules of online privacy and sensitivity to the issue. Parents need to create an environment of trust and reassure the child that he/she can approach either of them with any issue. Furthermore, parents are encouraged to communicate and agree on boundaries regarding posting content on social media and parental filtering measures.

Moreover, the handbook covers the case of a child who is a victim of cyberbullying. ‘Red flag’ behaviours are highlighted which indicate that the child is

⁵³ http://www.lider.szs.pl/download/zero_tolerancji.pdf

likely to be the victim of some form of abuse. Such behaviours include truancy, avoiding contact with peers, giving up favourite activities, mood swings, worsening behavioural problems, nervousness. According to the guidelines, the right response in such a situation is to remain calm, find out the facts and reassure the child that he/she is in a safe environment. If the abuse is indeed real, and action plan should be drawn out with the involvement of the child. This should include gathering evidence (e.g. messages from the perpetrator, contact details). This is a key factor as online materials could be easily hidden or deleted. Once the evidence of cyberbullying has been saved, the incident should be reported to the service provider. If the identity of the perpetrator is known, the parents of the child and the educational institution should be contacted and, if necessary, a police report should be made, depending on the circumstances of the case. The handbook considers that in most cases cyberbullying does not reach the level that would justify police intervention and – if handled well – can be remedied at institutional level.

Children may be victims of cyberbullying, but perpetrators too. The handbook covers the case a child involved in cyberbullying on the perpetrator's side. In this case too the most important element of action is to communicate with the child and to find out the reason behind his/her actions. Research shows that in most cases children on the perpetrator side are not aware of the consequences of their actions. In addition to explaining how cyberbullying is wrong and how serious the consequences can be, parents should offer them the possibility of reparation.

Furthermore, the handbook lists useful telephone numbers and websites when one has to deal with cyberbullying. This handbook is the most precise guide for civilians.

There are other materials that provide assistance. There is one aimed specifically at teachers⁵⁴. This particular guidebook draws attention to the importance of working with parents and lists programmes that can work in the context of prevention. The importance of good internal procedures and training for both students and teachers is also highlighted. Several NGOs are also taking on the organisation of training courses to prevent cyberbullying. One of these is the programme 'Stop cyberprzemoc'⁵⁵ of the Centre for Prevention and Addiction Treatment. However, these programmes bear little relevance to the legal background of cyberbullying, as these approach the issue differently.

54 <https://it-szkola.edu.pl/publikacje,plik,71>

55 <http://www.profilaktyk.info/cyberprzemoc.html>

5. The Responsibility of Service Providers and Institutions

The Polish provisions on the rules on the internet are set out in the Civil Code and the Electronic Services Act (Ustawa o świadczeniu usług drogą elektroniczną)⁵⁶, which also transposes the relevant EU rule, the e-commerce directive. In addition to the constitutional provisions on freedom of expression and the prohibition of censorship, Chapter 5 of the Press Law refers to rules on sprostowanie (correction), which also apply to press content published in electronic form. Accordingly, the editor of a press product published in electronic form is obliged to carry out the correction within 3 days. Currently, there is no specific legislation that regulate the liability of service providers for hate speech or individuals for cyberbullying. There was a intention to do so in late 2020 and early 2021, but the process has been put on hold.

On 17 December 2020, the Department of Justice announced⁵⁷ that social media service providers will be regulated. The bill was originally planned to be finished in mid-2021. However, in connection with certain political events (e.g. blocking of Twitter and Facebook accounts of former US President Donald Trump), on 1 February 2021 the draft law aimed at protecting freedom of expression in online social media services (Ustawa z dnia 2021 r. o ochronie wolności słowa w internetowych serwisach społecznościowych – hereinafter: Draft) was published.⁵⁸ In the following sections the contents of the Draft will be analysed as – while not entering into force – it still remains an important indicator of legislative intent.

The issue of social media regulation has been on the agenda in Poland for years. Many journalists have complained⁵⁹ that Facebook has arbitrarily blocked their profiles or deleted content they have shared. On 23 September 2019, the President of the National Media Council filed a lawsuit against Facebook at the Warsaw District Court,⁶⁰ claiming that the social media provider violated the freedom of expression guaranteed by the Constitution by restricting the availability of content posted by Facebook. This action has highlighted the difficulties of dealing with disputes and objections against Facebook and social

⁵⁶ Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20021441204/U/D20021204Lj.pdf>

⁵⁷ The announcement was made at a press conference.

⁵⁸ <https://www.gov.pl/web/sprawiedliwosc/zachecamy-do-zapoznania-sie-z-projektem-ustawy-o-ochronie-wolnosci-uzytownikow-serwisow-spoecznościowych>

⁵⁹ <https://www.ordoiuris.pl/dzialalnosc-instytutu/znani-dziennikarze-w-obronie-wolnosci-slowa-w-mediach-spoecznościowych>

⁶⁰ <https://bydgoszcz.tvp.pl/44519306/skladam-pozew-krzysztof-czabanski-przeciw-cenzurze-w-internecie>

media providers. The Warsaw District Court had to serve the action in Ireland, as Facebook's local subsidiary is responsible for its European operations. It is questionable whether Facebook has undertaken to take the case to the Polish courts, as no other information is available on the proceedings, which are presumably still ongoing.

The Draft is therefore a response to this obvious regulatory need. According to the Preamble of the Draft, it was born out of the recognition that freedom of expression – as a fundamental constitutional right – is indispensable to the search for truth, the functioning of a democratic state, and respect for freedom of expression and human dignity.

The Draft regulates social media service providers with at least 1 million registered users. The aim is to strengthen the protection of human rights on these platforms and supervise social media services. The scope of the regulation is explicit and narrow. In contrast, in Ireland or the UK a similar provision covers a much wider range of internet services. The Draft defines social media services (*internetowy serwis społecznościowy*) and service providers (*usługodawca*). Social media services are recognized as electronic services that allow users to share content, the recipient of which is another user or the public (and which have at least 1 million registered users).

The Draft contains comprehensive rules. It regulates:

- monitoring social media service providers to ensure that users' freedom of expression and their right to real information are guaranteed;
- the liability of service providers for illegal content (including hate speech);
- the obligations of service providers to guarantee freedom of expression and access to truthful information;
- the rules for a mandatory user-initiated complaints mechanism to be operated by service providers for reporting illegal content (i) and for reporting violations of freedom of expression.

The Draft sets out in detail the obligations of service providers, which include general (i) and ad hoc (ii) reports of obligations to enhance transparency. A service provider that receives more than 100 notifications (complaints concerning illegal content, restriction of content or users) in a calendar year must provide a report (*sprawozdan*) on how the notifications were handled. The report must be made available on social media in an accessible place, directly and permanently. The service provider shall apply to the President of the Electronic Communications Authority for the report to be published in the official bulletin of the Electronic Communications Authority (*Dziennik Urzędowy Urzędu Komunikacji*

Elektronicznej)⁶¹. The President of the Electronic Communications Authority shall publish the report immediately. In the case of ad hoc reporting obligation, social media providers shall prepare a report containing the procedures applied so far in the fight against fake news and the dissemination of illegal content.

The Proposal introduces a new legal instrument to ensure effective protection of individual rights. The so-called ‘blind action’ (*ślepy pozew*) allows a person to bring a claim for an infringement of personality rights in the online space against an unknown defendant. The action can be brought without knowing the defendant’s personal details, by providing a link to the infringing content, the date and time of publication and the infringing user account. Chapter 8 of the Draft aims to amend the rules of the Civil Code and the Civil Procedure Code to introduce this new legal instrument. The possibility to initiate a ‘blind action’, as proposed by the Polish Ombudsman, will be introduced in the Polish legal order along the lines of the John Doe lawsuit⁶², which is known in the United States of America.

The Draft does not impose a general obligation on service providers to monitor content, but they must remove unlawful content (*treści o charakterze bezprawnym*) and criminal content (*treści o charakterze przestępnym*) on notification and on the instruction of the prosecutor.

Furthermore, a transparent and efficient procedure for dealing with complaints from users should be established and made available in Polish. The rules of the social media service (*regulamin internetowego serwisu społecznościowego*) must comply with Polish law and should also be made available in Polish. The rules should include a detailed description of the notification procedure. If the service provider does not uphold the complaint against the illegal content, it shall inform the user of the possibility of initiating civil proceedings or, in the case of suspected criminal offences, of filing a complaint.

The Draft defines unlawful content and specifically highlights content that constitutes a criminal offence. Unlawful content is content that

- violates privacy rights,
- is considered fake news,
- violates the requirement of fairness,
- promotes or disseminates violence, suffering and humiliation.⁶³

⁶¹ Available: <http://edziennik.uke.gov.pl/actbymonths>

⁶² The name for a type of suit brought against unknown defendants in US procedural law.

⁶³ Art.3.8) “*treści o charakterze bezprawnym – rozumie się przez to treści naruszające dobra osobiste, dezinformację, treści o charakterze przestępnym, a także treści, które naruszają dobre obyczaje w szczególności rozpowszechniają lub pochwalają przemoc, cierpienie lub poniżenie*”.

This also includes content that constitutes a criminal offence in accordance with the Criminal Code (Kodeks karny). These are typically incitement to hatred, hate speech, offences against the State, offences against life or health, offences against liberty, offences against freedom of conscience and religion, offences against sexual autonomy and integrity, offences against State and local government bodies, offences against the fairness of elections, offences against public order and disobeying military orders.⁶⁴ In this case the Draft allows the public prosecutor to request the service provider or its representative to provide information or data that would allow the identification of the user who made the criminal content available. The prosecutor shall immediately order the service provider to remove the content if the content is one of pornographic nature involving minors or calls for the commission of terrorist acts, advocates terrorist acts or the long-term availability of the content has the potential to cause significant harm or to have an irreversible effect. The decision of the prosecutor shall be implemented immediately. The decision of the public prosecutor may be challenged (zażalenie) before the district court (sąd rejonowy).

According to the conditions set forth by the Draft, the provider may be fined if the representative of the provider does not investigate the notification or if he/she does not carry out the prosecutor's order. The fine may be imposed on both the social media company and the representative of the social media company, and ranges from 50,000 to 50,000,000 złoty (€11,000 to €11,000,000).

The Draft also contains explicit provisions in the event that a social media service provider blocks a user's profile (ograniczenie dostępu do profilu użytkownika) or makes content posted by the user on social media inaccessible (ograniczenie dostępu do treści).

There is a new, ongoing legislative project which concerns hate speech towards LGBTQ-persons.⁶⁵ The amendment to the Code of Civil Procedure is intended to allow a person affected by cyberbullying to file a so-called blind claim with the court, and the court to require the website administrator to disclose the IP address of the perpetrator. At the time of the closure of the manuscript, the draft was in the process of being submitted to the legislature. Nevertheless, it is important to note that crucial legal innovation is on the brink.

64 Art.3.7) "treści o charakterze przestępnym – rozumie się przez to treści, które pochwalają lub nawołują do popełnienia czynów zabronionych, określonych w artykułach: 117-119, 127-130, 133, 134-135, 137, 140, 148-150, 189-189a, 190a, 194-204, 222-224a, 249-251, 255-258, 343 ustawy z dnia 6 czerwca 1997 r. – Kodeks karny (Dz. U. z 2020 r. poz. 1444 i 1517) lub realizują znamiona czynu zabronionego."

65 <https://www.rp.pl/prawo-karne/art40270611-bedzie-zakaz-hejtu-wobec-osob-lgbt-projekt-ustawy-juz-gotowy>

As of now, given that cyberbullying is not regulated in Poland, no specific rules concerning liability issues can be established. This includes the liability of educational institutions and employers. However, according to the Polish Education Act (*Prawo oświatowe*)⁶⁶, schools are obliged to ensure a safe environment for children and to intervene if necessary. The school also has a duty to cooperate with parents. The intervention should include investigating the circumstances of the incident that threatens the safe environment and preserving evidence. Furthermore, educational institutions are obliged to notify the parents of all pupils involved, use the disciplinary means at its disposal in accordance with Polish law and school rules and refer to the police if necessary. Workplaces – such as educational institutions – also have a duty to provide a safe working environment, and their responsibilities are similar to those of educational institutions.

Pursuant to the Code of Criminal Procedure⁶⁷, anyone who becomes aware of a crime that has been committed must notify the prosecutor's office and the police. Informing the authorities of a crime committed is not only a right but also a civic duty. Witnesses or victims have several possibilities to refer to the authorities. If the notification is made in writing, the whole case must be described in the notification form laid down by law and the letter sent to the prosecutor's office. In case of a report made in person, one must go to the police station and make a verbal report. The police is obliged to document this report. The authorities may refuse to investigate, but in any case the report must be accepted by both the public prosecutor's office and the police. The prosecutor must issue a decision to investigate or refuse to investigate within a maximum of 30 days.

Summary

In Poland, neither hate speech nor cyberbullying is regulated separately or specifically. Furthermore, no precise definition of the term has been provided. The provisions of the Polish Constitution, the Civil Code, the Criminal Code and the Code of Criminal Procedure are authoritative, as well as judicial practice and guidelines and manuals, which consider both hate speech and cyberbullying unacceptable, with variations on when each act becomes a criminal offence. The lack of regulation and the ambiguity of the legislation is clear in both law

⁶⁶ <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19910950425/U/D19910425Lj.pdf>

⁶⁷ <https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970890555/U/D19970555Lj.pdf>

enforcement and criminology. It is important to note that according to the legal literature, Polish jurisprudence is critical of the current legislation, which does not provide a real solution for the issue of cyberbullying.⁶⁸ A 2017 report by the State Audit Office, which assessed cyberbullying as a real and a grave problem. In this environment it is hard to imagine that the legislation is yet to take action against cyberbullying and online hate speech. The lack of earnest response provides a barrier for prevention, therefore a long-term solution is only possible when the legislation will reflect the seriousness of online crimes.

However, it is clear that there is a legislative need for online hate speech regulations and a lot might change in the near future.

68 Las.

Bibliography

- Bedrosova, M., Machackova, H., Šerek, J., Smahel, D., Blaya, C. (2022) 'The relation between the cyberhate and cyberbullying experiences of adolescents in the Czech Republic, Poland, and Slovakia', *Computers in Human Behavior*, Volume 126.
- Bojanowski T (2021) 'Wybrane prawnokarne aspekty mowy nienawiści w kontekście standardów ochrony wolności słowa', DOI: 10.32041/pwd.4710
- Budyn-Kulik, M (2020) 'Nowe znamiona nękania z Art. 190a § 1 Kodeksu karnego', *Palestra*, 2020/9. pp. 22–34.
- Ćmiela, S (2014) 'Cyberbullying legislation in Poland and Selected EU Countries', *Procedia – Social and Behavioral Sciences*, 109, pp. 29–34.
- Janczukowicz, K. (2016) Stalking w orzecznictwie sądów, LEX/el.
- Kania, M (2020) Stalking a windykacja, ABC. [Online] [https://sip.lex.pl/#/ publication/470025267](https://sip.lex.pl/#/publication/470025267)
- Las, Katarzyna (2020) 'Odpowiedzialność karna za zjawisko cyberprzemocy w świetle prawodawstwa polskiego', *Rocznik Bezpieczeństwa Międzynarodowego*, 14(1), 256–277. <https://doi.org/10.34862/rbm.2020.1.15>
- Lipiński, K. (2021) 'Art. 190a [Uporczywe nękanie. Kradzież tożsamości]' in Giezek, J. (ed.) *Kodeks karny. Część szczególna. Komentarz*. Warsaw, Wolters Kluwer.
- Marciniak, J (2020) Praktyka sądowa dotycząca zjawiska mobbingu, ABC. [https:// sip.lex.pl/#/publication/469911290?keyword=Poni%C5%BCenia](https://sip.lex.pl/#/publication/469911290?keyword=Poni%C5%BCenia)
- Mozgawa, M. (2021) Kodeks karny. Komentarz, WKP [https://sip.lex.pl/#/ publication/151396710/kodeks-karny-komentarz](https://sip.lex.pl/#/publication/151396710/kodeks-karny-komentarz)
- Nask Academy (n/a) Cyberprzemoc, Włącz blokadę na nękanie, Poradnik dla rodziców
- Obserwatorium Językowe Uniwersytetu Warszawskiego (n/a) 'cyberprzemoc' <https://nowewyrazy.uw.edu.pl/haslo/cyberprzemoc.html>
- PWN (n/a) 'Udręczenie' <https://sjp.pwn.pl/szukaj/Udr%C4%99czenie.html>
- Wieczorkowski, J., Suwińska, A. (2021) 'Mowa nienawiści w mediach społecznościowych', *Zarządzanie Mediami*, 9(4), pp. 681–693.

IX. TO HATE OR NOT TO HATE – REGULATION OF HATE SPEECH AND CYBERBULLYING IN ROMANIA

PÁL SZENTPÁLI-GAVALLÉR

1. Introduction

According to the Constitution of Romania (hereinafter referred to as: Constitution) the authorities respect and protect family and private life.¹ On the basis of constitutional regulations, freedom of thought, opinion or religious belief may not be restricted in any form, and no one may be forced to accept an opinion or adopt a religious belief contrary to his or her conviction, and according to the Constitution defamation of country and nation, incitement to war of aggression, national, racial, class or religious hatred, incitement to discrimination, territorial separatism or public violence, as well as obscene manifestations contrary to public decency are prohibited by law.² Freedom of conscience is guaranteed and must be exercised in a spirit of tolerance and mutual respect. Religious denominations are free and organized according to their own statutes and in compliance with legal conditions. In relations between religious denominations, it is forbidden to carry out any form, means, or acts of incitement to religious hatred.³

1 Constitution Art. 26.

2 Constitution Art. 1., 6., 16. and 30.

3 Constitution Art. 29.

2. Regulatory issues of hate speech

Romania is considered a young democracy, which also means that its legal framework for the protection of human rights is still rather weak and that the need to combat discrimination and hate-based phenomena is not taken up either at the level of state decision-making or within the public law system of the state in general, this situation of being a young democracy inevitably entails, at least in certain respects, the absence or inadequacy of data.⁴

2.1. Definition of hate speech in Romania, related case law

In respect to the constitutional regulations – dogmatically – Act No. 286. of 2009. on the Romanian Criminal Code (hereinafter referred to as: Criminal Code) establishes a number of specific criminal offences relating to such as incitement to hatred or discrimination, according to which incitement to hatred or discrimination is defined as any incitement to hatred or discrimination by the public against a group, which act is punishable by imprisonment lasting between six months and three years or is punishable by a fine,⁵ and the Romanian legislator regulates in the Criminal Code the case of committing a crime on the grounds of hatred among aggravating circumstances and factors.⁶ Based on the Criminal Code the incitement to commit the crime of genocide, committed directly in public, shall be punishable by imprisonment for a term of two to seven years and by disqualification from exercising certain rights.⁷ And another important regulation is Emergency Decree No. 31. of 2002., which prohibits fascist, racist and xenophobic organisations and symbols.⁸

In connection with the above another relevant Romanian legislation includes:

- Law No. 157. of 2018. on measures to prevent and combat anti-semitism,⁹
- Law No. 2. of 2021. on measures to prevent and combat anti-gypsyism,¹⁰

4 An overview on hate crime and hate speech Country profile: Romania, 2017. p. 6.

5 Criminal Code Art. 369.

6 Criminal Code Art. 77.

7 Criminal Code, Art. 438. Section (4).

8 Hate crime recording and data collection practice across the EU, FRA, 2018. p. 78.

Government Emergency Ordinance No. 31/2002. on the prohibition of fascist, legionary, racist or xenophobic organisations, symbols and acts and the promotion of the cult of persons guilty of crimes of genocide against humanity and war crimes Art. 3-4.

9 Law No. 157 of 2018 on some measures to prevent and combat anti-Semitism.

10 Law No. 2. of 2021. on measures to prevent and combat anti-gypsyism.

- Law No. 202. of 2002. on equal opportunities for women and men,¹¹
- Law No. 504. of 2002. on broadcasting.¹²
- Government Ordinance No. 137/2000. concerning the prevention and sanctioning of all forms of discrimination (hereinafter referred to as: Government Ordinance No. 137/2000.).¹³

In Romanian law it is an important factor, that the following terms and expressions are very well defined:

- anti-gypsyism means both the perception of Roma expressed as hatred against them and verbal or physical manifestations, motivated by hatred against Roma, directed against Roma people or their property, institutions, NGOs, leaders of Roma communities or their places of worship, traditions and the Romani language;
- anti-gypsyist organisation means any group consisting of three or more persons, operating temporarily or permanently, with the aim of promoting anti-gypsyist ideas, concepts or doctrines. This category may include organisations with or without legal personality, political parties and movements, associations and foundations, companies regulated by the Companies Act No. 31. of 1990.;
- symbols of anti-gypsyism shall mean: flags, emblems, badges, uniforms, slogans, greetings, and any other such symbols, which convey ideas, concepts or doctrines promoting anti-gypsyism;
- anti-gypsy material means: images, text messages, audio-visual content, and any other such representations, which convey ideas, concepts or doctrines promoting anti-gypsyism.¹⁴

In relation to Law No. 2. of 2021. on measures to prevent and combat anti-gypsyism and according to a 2009 study, deliberate and organised hate speech and incitement to violence against Roma and Sinti have been observed in several countries, including Romania. It is easy to identify those behind the acts in question, as anti-Roma hate speech has been openly used as a tool by far-right political parties, extremist organisations or movements.¹⁵

11 Law No. 202. of 2002 on equal opportunities for women and men.

12 Law No. 504. of 2002 on broadcasting.

13 Ordinance No 137 of 2000 on the prevention and punishment of all forms of discrimination.

14 Law No. 2. of 2021. on measures to prevent and combat anti-gypsyism Art. 2.

15 The Extreme Right and Roma and Sinti in Europe: A New Phase in the Use of Hate Speech and Violence? 2009, p. 6.

There were measures taken in Romania to promote equality of opportunity and treatment between women and men and to eliminate all forms of discrimination based on sex, and these laws shall apply in the public and private sectors, in the fields of employment, education, health, culture and information, politics, participation in decision-making, the provision of access to goods and services, the establishment, equipping or extension of a business or the commencement or extension of any other form of self-employed activity, and in other areas regulated by special laws. All these institutions listed in the law with powers in the field of equal opportunities and equal treatment of women and men, each for its field of activity, shall be obliged to bring by all appropriate means to the attention of the persons concerned the provisions adopted under the law, together with the relevant Romanian provisions already in force.¹⁶

According to the Law No. 504. of 2002. on broadcasting it is forbidden to broadcast programs that contain any form of incitement to hatred on the grounds of race, religion, nationality, sex or sexual orientation.¹⁷

The Government Ordinance No. 137/2000. provides that the principle of equality among citizens and the elimination of all privileges and discrimination shall be guaranteed in Romania, in particular with regard to the exercise of the following rights:

- the right to equal treatment before courts and any other jurisdictional bodies;
 - the right to personal security and to be granted state protection against violence;
 - mistreatment perpetrated by any individual, group or institution;
 - political rights, namely electoral rights, the right to take part in public life; and
- the right to access to public positions;
- other civil rights, in particular:
 - (a) the right to freedom of movement and of choosing one's residence;
 - (b) the right to leave and return to one's country;
 - (c) the right to obtain the Romanian citizenship;
 - (d) the right to marry and to choose one's partner;
 - (e) the right to property;
 - (f) the right to inheritance;
 - (g) the right to freedom of thought, conscience and religion;
 - (h) the right to freedom of expression and opinion;

¹⁶ Law No. 202. of 2002. on equal opportunities for women and men Art. 2. Sections (1)-(2).

¹⁷ Law No. 504. of 2002. on broadcasting Art. 40.

- (i) the right to freedom of peaceful meeting and association;
- (j) the right to file a petition;
- economic, social and cultural rights;
 - (a) the right to work,
 - (b) the right to freely choose an occupation,
 - (c) the right to fair and satisfactory working;
- the right to protection against unemployment, to equal pay for equal work, to fair and satisfactory wages as far as:
 - (a) the right to establish and to join trade unions;
 - (b) the right to housing;
 - (c) the right to health, medical assistance, social security and social services;
 - (d) the right to education and to professional training;
 - (e) the right to take part in cultural activities in conditions of equality;
- the right of access to all public places and services.¹⁸

In parallel with the Romanian constitutional regulation, according to Act No. 51. of 1991. on National Security (hereinafter: National Security Act), no one may be prosecuted in Romania for freely expressing his or her political opinion, nor may he or she interfere in private and family life, or private correspondence or communication if no act has been committed which, according to the National Security Act, which endangers national security and cyberspace.¹⁹

It is clear from the above that the Romanian legislation is implemented at two legislative levels and is quite specific.

The European Council's Committee of Ministers' definition that hate speech should be understood as any form of expression that spreads, incites, supports or justifies racism, xenophobia, antisemitism or other forms of hatred based on intolerance, including intolerance expressed by aggressive nationalism and ethnocentrism, towards minorities, migrants and persons with an immigrant background discrimination and hostility.²⁰ Another scientific research on the operation of the RMDSZ (UDMR)²¹ in Romania has shown that the Hungarian (and Szekler) minorities in Transylvania are also the subject of incitement to hatred in Romania.²² Romanian Criminal law provisions corresponding to ECRI's General Policy Recommendation No. 7. on national legislation to combat

18 Government Ordinance No. 137/2000. Art. 1. Section (2).

19 Act No. 51. of 1991 on the national security of Romania Art. 3.

20 Meza, 2016, p. 58.

21 In English: Democratic Alliance of Hungarians in Romania.

22 Meza-Vincze-Mogoş, 2018, p. 41.

racism and racial discrimination can be found in the Criminal Code and the Emergency Government Ordinance No. 31/2002. on prohibiting organizations of a fascist, racist and xenophobic character and the glorification of those found guilty of crimes against peace and humanity. ECRI takes positive note of the amendments to the Emergency Government Ordinance No. 31/2002. in 2015, which enlarged its scope of application by prohibiting legionary symbols and acts related to the Holocaust, including on the territory of Romania. ECRI also welcomed the adoption of specific criminal legislation²³ in July 2018 regarding measures to prevent and combat antisemitism.²⁴

With regard to freedom of speech as a counterpoint to hate speech, the Constitution stipulates that the law prohibits defamation of country and nation, incitement to war of aggression, national, racial and religious hatred, discrimination,²⁵ territorial separatism or public violence, and obscene expressions contrary to good morals.²⁶ With this in mind, the legislature guarantees everyone complete and inviolable freedom of expression without fear of government retaliation or censorship of such information. The regulation explicitly states in relation to censorship: ‘all censorship is prohibited’. In this connection it is necessary to indicate that the constitution prohibits not only government censorship, but also any other kind of censorship. According to an expanded interpretation of this, social media gatekeepers can also violate freedom of expression: censoring users.²⁷ Freedom of expression is therefore restricted by morality under the provisions of the Constitution. The new Civil Code, adopted in 2009, also contains relevant provisions: it establishes the right to freedom of expression,²⁸ according to which everyone has the right to freedom of expression. The law also sets limits on the right to freedom of expression, including:²⁹

- violations permitted by law or international conventions do not constitute a violation of the rights granted,
- the exercise of constitutional rights and freedoms in good faith and in compliance with human rights and international conventions does not constitute a violation of the rights guaranteed.³⁰

23 See: Law No. 157. of 2018. on measures to prevent and combat anti-semitism

24 <https://rm.coe.int/fifth-report-on-romania/168094c9e5>, p. 11.

25 Cf.: Varga, 2019, p. 303.

26 Constitution Art. 30.

27 Cf.: Voinea, 2015, p. 173., p. 177.

28 Civil Code Art. 70.

29 Cf.: Dr. Casarosa, 2020, pp. 70–71.

30 Voinea, 2015, p. 177.

The right to privacy is defined in the new Civil Code,³¹ according to which everyone has the right to respect for his private life, and the right to privacy is also protected by the Constitution. The explanation and extension of this right is regulated by the same law, no one should interfere with private life, personal or family life, place of residence, or private correspondence without their consent or compliance with the restrictions contained in the new Civil Code, since this provides extra protection for privacy, be it personal or family life, but also extends to the household of individuals and correspondence of individuals,³² thus, their home and postal correspondence are inviolable. The law, providing additional protection, states that it is forbidden to use correspondence, manuscripts or other personal documents, as well as private information of a person in any way, without the consent of that person or without respecting the limits set out in the new Civil Code.³³

Based on a Romanian-language report hate crimes are offences punishable under criminal law that are determined by the offender's feelings towards a particular community, as determined by a common characteristic, and not personally towards the victim. Criminal law uses the term crime for reasons related to a criterion of discrimination (on grounds of race, nationality, ethnicity/ethnic origin, language, religion, gender/sex, sexual orientation, opinion, political affiliation, beliefs, wealth, social origin, age, disability, chronic non-communicable disease or HIV/AIDS infection).³⁴

According to a report published by the European Union (hereinafter referred to as: EU), decisions on audiovisual content regulated by the National Audiovisual Council and issued in legislative form generally cover the protection of interests, which includes the protection of children's rights and the psychological integrity of adults. One significant case concerning the limits of freedom of expression in Romania is worth mentioning, when OT SRL, the owner of a television channel (OTV), was fined administratively and obliged to publish the sanction by the Romanian regulatory authority, the National Audiovisual Council (hereinafter referred to as: NAT). The company was fined for showing footage of a former Romanian prime minister being photographed nude in the locker room of a fitness room during a television show. The footage was made by another television channel, which also showed the footage. The presenter and his guest made various ironic and offensive comments about the former prime

³¹ Civil Code Art. 71.

³² Civil Code Art. 74.

³³ Civil Code Art. 74.

³⁴ <https://www.crj.ro/wp-content/uploads/2023/02/Raport-Infractiuni-motivate-de-ura-2021-2022.pdf>

minister's appearance. NAT concluded that television violated the protection of fundamental rights, such as dignity, privacy, honour, reputation, personality rights and image. The television ignored the fact that the footage shown was not in the public interest, but concerned only Mr E.B.'s private life. In its judgment on a separate appeal by OTV, the Supreme Court of Cassation and Justice dismissed the appeal and upheld the decision of the Bucharest Court of Appeal at first instance, ruling that the sanctions imposed by NAT had been lawfully applied. The Court assessed the right to dignity, private and family life and the right to good repute in balance with journalists' freedom of expression. With reference to freedom of expression, the applicant based its reasoning on the provisions of both Article 10 of the European Convention on Human Rights (hereinafter referred to as: Convention) and Article 11 TFEU. The Court held that the applicant's argument that the images had already been broadcast by other television channels and that OTV had only rebroadcast them could not justify OTV's action, since each television channel could be held liable for the recordings it showed, and that the Court rejected the applicant's argument that the public interest justified the broadcasting of the recordings, since „the nude pictures of E.B. and the offensive remarks are not his physical features of any public interest...”³⁵

2.2. Statistics on hate speech in Romania

The OSCE noted that Romania has not reported statistics on hate crimes to the OSCE since 2018, but reports a high number of cases in the period 2021-2023. In addition, the OSCE indicated that Romania would benefit from increasing the awareness and capacity of criminal and judicial officials in relation to hate crimes. The Romanian statistics are as following in the last years:³⁶

Year:	Hate crimes recorded by police:	Prosecuted:	Sentenced:
2023	95	252	239
2022	59	129	16
2021	7	54	128

Table 4. Hate crimes in Romania³⁷

35 Casarosa, 2020, pp. 70–71. Decision 359/2014 of the Supreme Court of Cassation and Justice of 28 January 2014.

36 <https://hatecrime.osce.org/romania?year=2020>

37 <https://hatecrime.osce.org/romania?year=2020>

According to the Council of Europe's 2019 report on Romania,³⁸ racist and intolerant hate speech is a widespread problem in public and online discourse, in relation with Roma, the Hungarian (or Szekler) minority, LGBTQ-linked people and the Israelite community being the main targets. There are also sporadic violent attacks against these groups or their property. In relation to the above mentioned problems an opinion on the operation of the RMDSZ in Romania has shown that the Hungarian (or Szekler) minorities in Transylvania are also the subject of incitement to hatred in Romania.³⁹

3. About Romanian cyberbullying

As an EU study shows, cyberbullying is not a separate crime in Romania. Depending on the nature and effects of aggression, the offense is punishable under the Criminal Code or other legislation.⁴⁰

Romania had the highest rate of cyberbullying, similarly to other Eastern European countries. The percentage of Romanian adolescents abused online was much higher than indicated by the EU Kids Online study. In Romania, the use of the internet and social media platforms has risen sharply in recent years. The underestimation of risks by parents and the lack of digital skills of parents may have contributed to the high rate of victims of cyberbullying. In Romania, compared to the steadier and much earlier growth in internet usage in the other European countries studied, the sudden increase in internet usage has resulted in a large technological gap between the parents' generation and the younger generations. In addition, the lack of a legislative framework to protect children online in Romania and the current lack of integration of ICT elements⁴¹ into education limit the promotion of online safety and awareness of online risks.⁴² The previous opinion is confirmed by a study according to which young Romanians and Estonians reported the highest prevalence rates of cyberbullying.⁴³ Roma were the most frequently referred to on internet social media platforms⁴⁴ (such

³⁸ Meza-Vincze-Mogoş, 2018, p. 41.

³⁹ Council of Europe: ECRI report on Romania, 2019, p. 9.

⁴⁰ Chateau, 2016, p. 143.

⁴¹ ICT refers to information and communication technologies. http://tanarblog.hu/attachments/2787_PILAkademia_bevezeto.pdf

⁴² Athanasiou-Melegkovits-Magoulas-Tzavara-Richardson-Greydanus-Tsolia-Tsitsika, 2018. <https://bmcpublihealth.biomedcentral.com/articles/10.1186/s12889-018-5682-4>

⁴³ Baldry-Blaya-Farrington, 2018, p. 6.

⁴⁴ Baldry-Blaya-Farrington, 2018, p. 6.

as Facebook) due to the use of the term ‘țigan/i’,⁴⁵ and the most frequent occurrence of the term was related to degrading language use, followed by semantic word combinations related to debility.⁴⁶

Romanian criminal law deals in detail with fraud and computer crimes committed through computer systems and electronic means of payment, bullying and cyberbullying conduct in Romania are not regulated in the Criminal Code, but in Decree No. 4343/2020. it is regulated.⁴⁷ However, criminal law contains a number of offences that correspond to an act or form of intimidation, such as harassment or threats.⁴⁸ Romanian legislation applies the definition of harassment and its conceptual elements are:

- intent,
- continuous or repetitive nature,
- making contact, intimidating, surveillance or otherwise causing disturbance.

Decree No. 4343/2020. on national education discusses psychological violence and bullying is the action or series of physical, verbal, relational and/or cyber actions, in a social context difficult to avoid, committed with intent, involving an imbalance of power, resulting in the violation of dignity or the creation of an intimidating, hostile, degrading, humiliating or offensive atmosphere, directed against a person or a group of persons and targeting aspects of discrimination and social exclusion, which may relate to membership of a particular race, nationality, ethnic group, religion, social or disadvantaged group or to beliefs, sex or sexual orientation, personal characteristics, action or series of actions, behaviour which takes place in educational establishments and in all places of education and training.⁴⁹

Aggravated harassment occurs when committed by a former spouse or partner or against the victim’s child. A relationship of subordination is not a condition for establishing the facts. The Criminal Code defines the offence of harassment as follows:

- an act committed repeatedly by an individual unlawfully or without a legitimate reason, which takes place at home, at work or in a place frequently visited by him, thereby inciting fear in others, is punishable by imprisonment of three to six months or by a fine,

45 In English: gypsies.

46 Meza, 2016, p. 69.

47 Criminal Code Art. 360–366.

48 Parti, 2016, p. 117.

49 Decree No. 4343/2020. Art. 1.

- fearful telephone calls or communications of an individual. According to above mentioned Romanian laws, committing harassment is punishable by imprisonment of one month to three months or by a fine if the act does not constitute a more serious crime.⁵⁰

The two main objectives of the National Strategy for the Protection and Promotion of Children's Rights 2014-2020 are relevant to cyberbullying:

- reducing children's exposure to the media and cyberviolence, and
- reducing violence between children by strengthening the legal status of public service providers.⁵¹

In relation to the above UNICEF defines cyberbullying as harassment using digital technologies that can occur on social media, messaging platforms, gaming platforms and mobile phones, a repetitive behaviour designed to scare or anger or shame individuals. Examples include the followings:

- spreading lies or posting embarrassing photos on social media,
- sending offensive messages or threats through messaging platforms, and
- sending vile messages to others on behalf of other people.

In connection with the above UNICEF definition, a new body, the Children's Board, was (in December 2019 initiated and)⁵² established in Romania at the beginning of 2020, thanks to which the Romanian Ombudsman and the Ombudsman for Children discussed priorities related to children in a consultation, as well as the role of the Ombudsman for Children in the coming years in order to promote and respect children's rights in Romania. In the margins of the consultation, UNICEF in Romania and the Romanian Ombudsman for the Rights of the Child issued a Memorandum of Understanding for the period 2020-2022. According to the statement of the Ombudsman, Renate Weber, the consultation of the Children's Board at the meeting and the memorandum signed with UNICEF are important steps towards achieving maximum capacity of the Ombudsman for the Child, which operates as an independent body within the Romanian Ombudsman's Office. In the Ombudsman's view, this organisation should become an organisation for the protection and promotion of children's rights, including through the continuous involvement of children. The institutional system of the Ombudsman for Children was established in 2018 and is coordinated by a deputy Romanian ombudsman and acts to promote and protect

⁵⁰ Criminal Code Art. 208.

⁵¹ Chateau, 2016, p. 145.

⁵² <https://www.unicef.org/romania/childrens-board-2020>

children's rights. The Ombudsman for Children is responsible for cooperating with child protection agencies and bodies and proposing measures to encourage children's participation in decisions affecting their lives. Gabriel Vockel, UNICEF Deputy Representative for Romania, believes that continuous monitoring of children's rights is necessary to ensure that the rights of all children are guaranteed and that public law policy is based on sound foundations. The Ombudsman for Children is a guarantor of respect for children's rights and a key partner in promoting children's participation, including through online and offline consultations. UNICEF provides technical support to the Ombudsman for Children to become a member of the European Network of Ombudsmen for Children (ENOC) and increase the capacity of specialist staff. Through the innovative U-Report platform supported by UNICEF, more than 1800 children and adolescents expressed their views on the role of the Ombudsman for Children. The Romanian Children's Board, established in 2019, is an organization composed of children of different ages, from all parts of the country, from different family backgrounds, included in the child protection system, of different ethnic origins and with diverse experiences, with thirty-two members. For most of them, this is the first time that their opinion has reached decision-makers. At EU level it is mentioned by the 8th European Forum on the Rights of the Child of 2013., so bullying has been defined as harassment or harassment of one child or more children when another child or young person or group of children or young people says unpleasant things to them, harassment when a child or young person is threatened, receives threatening messages, and similar situations may constitute harassment:⁵³ Chateau states that „The defining elements of cyberbullying are the same as for traditional bullying. However, cyberbullying requires additional specific features such as: the perpetrators' anonymity, the broad dissemination (messages are disseminated instantly and with an exponential reach), the repetition (the fact that events, photos and incidents posted online can be viewed and replayed over and over again). These characteristics make cyberbullying more dangerous than traditional bullying. Cyberbullying tends to be more common in countries where bullying rates are higher, which might suggest that cyberbullying is derived from regular bullying. Moreover, research shows that it is more widespread in countries with high rates of internet use. In contrary with this, Romania is one of the European countries mostly affected by cyberbullying although it has the lowest percentage of internet users according to 2015 statistics”⁵⁴ and „Perpetrators are generally known by the victims, being

53 Chateau, 2016, p. 22.

54 Chateau, 2016, p.141.

part of the victims' extended social group or attending the same schools as the victims. 19% of the 522 children aged 9-16 years old participating in the study by Net Children Go Mobile said that they aggressed someone online. Noticeably, the number of perpetrators was higher (25%) in children aged 15-16, but the proportion was also high (21%) among children aged 9-10 years. Similarly, the EU Kids Online II study showed the highest prevalence of perpetrators among children aged 15-16. A higher percentage of girls as online perpetrators than boys was recorded (5.2% versus 3.8%)."⁵⁵

Given the importance of the topic of improving the overall situation of women in everyday discourse and the issue of cyberbullying, it is also worth briefly presenting the case law in Romania. In connection with case-law, it is worth mentioning that case-law in which the applicant – Mrs Buturuga – lodged a complaint with the European Court of Human Rights (hereinafter: ECtHR) against her ex-husband, alleging that she had been a victim of domestic violence and that her ex-husband had threatened to kill her. The following month, she made a second complaint of threats and violence, the reason being that her husband tried to get her to withdraw the first complaint. Buturuga also requested an electronic search of the family computer, claiming that her ex-husband had unlawfully accessed her electronic folders and Facebook profile, copying her private conversations, documents and photographs, and then filed a third complaint for breach of confidentiality of correspondence. In February 2015, the prosecutor dismissed the complaint of domestic violence on the grounds that it was not serious enough to constitute a crime, and also dismissed the complaint of violation of privacy on the grounds that it was filed out of time. Before the ECtHR, Buturuga argued that his rights under the Convention, in particular the prohibition of torture and inhuman or degrading treatment under Article 3 thereof, and his right to respect for private and family life and correspondence under Article 8 of the Convention, had been violated. With regard to the investigation of the act of abuse, the Court found that the Romanian authorities did not examine the facts from the perspective of domestic violence. Their decisions were based on provisions of the Romanian Criminal Code that punish violence between individuals, rather than on provisions providing for harsher penalties for domestic violence. The ECtHR considered that the findings of the Romanian authorities were questionable as they had not identified the person responsible for the acts. As regards the investigation into the breach of the obligation to maintain privacy in relation to Buturuga's correspondence, the ECtHR pointed out that cyberbullying is currently a recognised aspect of violence

⁵⁵ Chateau, 2016, p. 142.

against women and girls and that cyberbullying can take many forms, including invasion of privacy, intrusion into the victim's computer, and recording, sharing and manipulation of data and images, including private data. The ECtHR also accepted Buturuga's argument that acts such as the illegal monitoring, illegal access to or saving of correspondence of a spouse could have been taken into account by the Romanian authorities when investigating cases of domestic violence, but in the present case the Romanian authorities ignored those grounds and rejected the woman's request for an electronic search of the family computer. The ECtHR considered that the Romanian authorities had taken a too formal position and failed to take into account many aspects of domestic violence. The ECtHR therefore considered that Romania had failed to fulfil its obligations under Articles 3 and 8 of the Convention and ordered the Romanian State to pay EUR 10000 to Buturuga.⁵⁶

4. Practice related to prevention

In Romania, the authorities (e.g. education inspectorates, Ministry of Education) collect data on violence in schools, but these data does not specifically relate to cyberbullying. Data on cyberbullying was collected at national level under the 2009–2011 Sigur.info programme and the 2012-2014 Net Children Go Mobile project in 2012–2014. Data on school violence, including bullying, is collected locally by school counselors and transmitted to the School Assistance Center at the regional level. The data was aggregated annually by the Ministry of Education. The National Council for Preventing and Combating School Violence is concerned with monitoring and coordinating the data collection process on school violence, including bullying, which takes place periodically at county and local level. Data on violence against children are managed by schools, the police and Directorate-General Social Support and Child Protection.⁵⁷

In Romania there are special initiatives, particularly in the non-governmental sector, which are primarily aimed at preventing cyberbullying. The non-governmental sector also provides a hotline where both children and adults can report illegal content in the online environment. In this respect school counselors and staff from School Assistance Centers are also involved in preventing and ending situations of violence in schools. Counsellors provide

⁵⁶ See: [https://hudoc.echr.coe.int/eng-press#{%22itemid%22:\[%22003-6635916-8811383%22\]}](https://hudoc.echr.coe.int/eng-press#{%22itemid%22:[%22003-6635916-8811383%22]})

⁵⁷ Chateau, 2016, p.147.

professional services in schools and monitor violent situations in schools by writing reports on their activities, thereby also taking into account the phenomenon of cyberbullying, which is a very good practice according to the author's opinion.⁵⁸

Romania's minister of education in 2022 announced that 1,200 new school counselor positions will be made available, which means a 50% increase from the number of the year 2022.⁵⁹ The above mentioned study,⁶⁰ indicates that the Ministry of Education, Research and Youth introduced a national strategy against violence in schools in 2007 as a beginning of the Romanian state's codification. The aforementioned strategy contains practical guides on preventing and dealing not only with violence in schools, but also with traditional – not cyber related – bullying, and according to Government Resolution 271/2013. on bullying and blackmailing, which may also cover cyberbullying.⁶¹

As mentioned in the previous chapter, UNICEF also helps improve the complaint-handling system. UNICEF and the Romanian Ombudsman are also working together to promote a culture of institutional accountability and transparency regarding in respect for children's rights in Romania, and within the scope of her or his duties, the Ombudsman for Children receives individual complaints lodged by children or their representatives concerning actions of public bodies in the fields of health, education, special protection of children, the application of measures not involving deprivation of liberty and any institution whose activities relate to the protection and promotion of children's rights. It also handles complaints about violations of children's rights and in this respect promotes children's rights.⁶² In relation to practice among the hotlines, the Children's Helpline Association is worth mentioning, a non-profit NGO that provides the only well-known free national helpline (*Telefonul Copilului*) for children and adolescents in Romania. The success story of the free helpline is entirely due to the pediatric and underage clients who turned to the hotline 116-111 in large numbers. More than 100,000 children and teenagers call the helpline every year, and tens of thousands of cases where children's lives put at risk have been resolved. Children and teens call the hotline 116-111 to express their fears, to talk about issues that directly affect them, and most importantly, to get help in an emergency. Social workers and psychologists at the Children's Helpline

⁵⁸ Chateau, 2016, p.145.

⁵⁹ See: <https://www.romania-insider.com/romaniyas-education-ministry-increase-number-school-counselors>

⁶⁰ Chateau, 2016, p.145.

⁶¹ Chateau, 2016, p.145.

⁶² <https://tinyurl.hu/z4ZD>

Association answer calls on 116-111 seven days a week. During its more than a decade of existence, the helpline has been called more than two million times.⁶³

Romani Criss, an NGO focused on Roma students, in cooperation with the Intercultural Institute, initiated measures to establish the status of school mediator in the Romanian education system. In 1998 and 1999, school mediators were trained and employed in a pilot project to tackle early school leaving called the Second Chance Programme.⁶⁴ The project was started by the Open Society Foundation and continued by the Education Center 2000+. In cooperation with Roma families and pupils, mediators⁶⁵ were tasked with providing support to Roma children and their families to improve their access to education, to ensure connectivity between schools and Roma communities and to provide consultation and counselling to members of the Roma community in order to prevent conflicts between families and schools, to raise awareness of the problems of Roma minority ethnicities and to promote the survival of multicultural values in an inclusive educational environment. According to the Strategy 2015–2020 for the integration of Romanian citizens belonging to the Roma minority, one of the priorities for combating school segregation of Roma and obstacles to access to education is to continue training programmes and employ school mediators in institutions where Roma children account for more than 15% of all enrolled children. In terms of results, there were 600 school mediators employed by the Romanian government in 2016, while 1680 school mediators were planned for 2020. School mediation is one of the important measures developed to support Roma students. Unfortunately, there is little information available about the impact of this measure, and the legal framework for the work of school mediators is quite vague, and the latter implies some uncertainty.⁶⁶ The researches have identified several forms of social exclusion that lead to an increase in the difficulties encountered in raising the educational level of the minority Roma, for example the pigeonholing of the Roma, according to which they participate in various actions leading to addiction (e.g. gambling, alcohol consumption). These stereotypes

⁶³ <https://www.116111.ro/ce-este-116111>

⁶⁴ Cf.: Country Report on Adult Education in Romania, 2011, p. 6.

⁶⁵ Three essential points which we come across again in most of the work done on the concept of mediation:

- the presence of a latent or open conflict between two parties,
- a request or an agreement by these two parties to appoint a neutral mediator,
- decisions taken which lead to changes in both camps.

<http://opeyroux.blogspot.com/p/question-of-roma-mediators-and-positive.html>

⁶⁶ Pop-Balea, 2016, pp.152–153.

can be more easily translated into intervention proposals than actually pointing out that child labor or the lack of the necessary minimum resources are the state's influence and that these areas and deficiencies should be treated as measures of the social protection net and institutions. The recommendations are first formulated in the area of legislation and the implementation of the legislation regulating the work of school mediators. It is important to emphasize that the creation of the professional environment necessary for the work of school mediators is one of the first aspects to be clarified before any other expectations are formulated in relation to this work. Moreover, at the macro level, the approach to Roma social inclusion has long since reached its limits, and the focus needs to be shifted to uncovering the structural roots and causes of ethnic inequalities, which calls for further policy measures and individual and family-based interventions. Second, with regard to scientific research in Romania, experts believe that qualitative research is needed to understand the situation of school mediators in schools and settlements and their work with Roma families and students. From a qualitative point of view, their interest would be to describe the process through which the school mediator fits into the context supporting the Roma students and families. Where do they place themselves and where do they place themselves in the binary division of supposed 'us' and 'them'? How do all these aspects affect their work? Finally, as Moi sets it out, the distribution and structure of power within society may explain how inequalities can be reproduced through strategies that fit already existing social structures and barriers.⁶⁷

As regards recent practice, it is worth noting that the Ministry of Education and Research in 2020 issued methodological rules, the purpose of which were:

- to help create a safe and positive climate in the educational establishment, based on respect for the person, non-discrimination, motivation for learning and ensuring the well-being of the pre-schoolers as well as the pupil in the educational establishment;
- to provide a working tool for professionals working with pre-school children and pupils in the education system, children's families, authorities responsible for the protection of children against violence, including psychological violence – bullying and with specialised service providers for the rehabilitation of child victims, witnesses and/or children with aggressive behaviour;
- to promote activities to prevent and combat all forms of bullying and cyberbullying in the pre-university education system;

⁶⁷ Pop-Balea, 2016, pp. 171–173.

- to prevent, identify, report and intervene in multidisciplinary teams in situations of psychological violence – bullying and cyberbullying.⁶⁸

Overall, in the opinion of the author, Romania's cyberbullying practice is progressive and evolving, although the regulation of cyberbullying against children still seems to be incomplete.

5. Liability of service providers and institutions

The issue of liability may also arise⁶⁹ if the information promoted through the use of meta-links infringes the rights of third parties or violates the provisions of Law No. 365. of 2002 on e-commerce (hereinafter referred to as: Law No. 365. of 2002). Law No. 365. of 2002 generally stipulates that service providers are subject to civil, criminal and misdemeanor liability laws and states that service providers are liable for information provided by them or on their behalf. This responsibility cannot be regarded as absolute, because it can only be exercised within certain limits.⁷⁰ The Authority shall order investigations to be carried out in accordance with this Law, ex officio or upon receipt of a complaint or referral by any person. The authorized inspection staff of the Authority or of any other public authority or public institution exercising powers with respect to the supervision of a particular sector or field of activity may require statements or any documents necessary for the performance of their duties, seal, take any registers, financial and commercial accounting and other records, and issue copies of the originals to the person subject to the investigation, or obtain copies, leaving the originals and shall also be authorized to carry out unannounced inspections, the results of which shall be recorded in a statement of findings, and to receive, when summoned or on the spot, information and supporting documents.⁷¹ Under certain conditions, the legislation makes it possible to declare contracts for information society services to be relatively null and void.⁷² However, the Law under discussion is considered an offence if it is not committed under conditions that constitute a criminal offence under criminal law, and the

68 Methodological Standards from 27 May 2020 Art. 2.

69 Cf.: Sorbán, 2019, pp. 85–91.

70 Law No. 365. of 2002 on electronic commerce Art. 11.

71 Law No. 365 of 2002 on electronic commerce Art. 17. Section (6)–(7).

72 Law No. 365 of 2002 on electronic commerce Art. 21.

service provider is punishable by a fine ranging from 1,000 to 100,000 RON if the legal conditions are met.⁷³

It is generally permissible to link to a third-party website that is unconditionally accessible to the public, provided that the third party's intellectual property rights and privacy rights are not infringed. If the third-party website is accessible to a specific category of the public (such as subscribers) and the link provided by the website facilitates direct access to the content of the third-party website, permission from the site owner is required.⁷⁴

Summary

In Romania, according to constitutional regulations, freedom of thought, opinion or religious belief may not be restricted in any form, no one may be forced to accept an opinion or adhere to a religious belief contrary to his or her convictions, and the law prohibits the desecration of the country and the nation. Any form of incitement to religious hatred is prohibited between religious denominations. The Romanian Criminal Code establishes a number of specific criminal offences, such as incitement to hatred or discrimination, according to which incitement to hatred or discrimination is defined as any incitement to hatred or discrimination by the public against a group, which act is punishable, as appropriate, by imprisonment or by a fine. In connection with the foregoing, in the author's opinion, another important regulation is Emergency Government Ordinance No. 31/2002., which prohibits fascist, racist and xenophobic organisations and symbols. Among the aggravating circumstances and factors, the Romanian legislator regulates in the Criminal Code the case when the crime is committed on the basis of race, membership of a national minority, religion, gender, sexual orientation, political opinion or party affiliation, economic status, social origin, age, disability etc. Other very important Romanian legislation includes:

- Law No. 157. of 2018. on measures to prevent and combat anti-semitism,
- Law No. 2. of 2021. on measures to prevent and combat anti-gypsyism,
- Law No. 202. of 2002. on equal opportunities for women and men,
- Law No. 504. of 2002. on broadcasting.
- Government Ordinance No. 137/2000. concerning the prevention and sanctioning of all forms of discrimination.

⁷³ Law No. 365 of 2002 on electronic commerce Art. 22.

⁷⁴ Lefter-Alexandru-Sima-Cosmina-Pachiu, 2018.

Outline of hate speech	
Specific criminal offences/factual situations	(a) incitement to hatred, (b) discrimination, (c) fascist, racist and xenophobic organisations, (d) fascist, racist and xenophobic symbols, (e) legionary symbols
Aggravating circumstances	(a) race, origin, (b) membership of a national minority, (c) language, (d) religion, (e) sexual orientation, (f) political opinion or party affiliation, (g) economic situation, (h) age, (i) disability, chronic disease, HIV/AIDS
Main targets	(a) Roma, (b) the Hungarian minority, (c) LGBTQ-linked people, (d) the Israelite community

Table 5. Outline of hate speech legislation in Romania⁷⁵

The research results show that the Romanian legislation is implemented at two legislative levels and is quite specific in relation to hate speech.

In the Romanian criminal law, crimes committed in the online space are not regulated, but computer crimes are regulated, and the regulation also establishes a number of specific criminal offences related to incitement to hatred, such as torture based on discrimination etc. According to the author's opinion, the latter raises the question of whether the Romanian legislation cannot be classified as casuistic.

In Romania, a new body, the Children's Board, was established at the beginning of 2020, thanks to which the Romanian Ombudsman and the Ombudsman for Children discussed child-related priorities in a consultation, as well as the role of the Ombudsman for Children in the coming years in order to promote and respect children's rights in Romania. This followed the establishment of the Ombudsman for Children in Romania in 2018, coordinated by a deputy Romanian ombudsman that acts to promote and protect children's rights. The Ombudsman for Children is responsible for cooperating with child protection agencies and bodies, and proposing measures to encourage children's participation in decisions affecting their lives. In order to ensure that all rights are guaranteed to all children and that public law policy is based on sound foundations, continuous

⁷⁵ Source: author's own editing.

monitoring of children's rights is necessary. The Ombudsman for Children is a guarantor of respect for children's rights and a key partner in promoting children's participation, including through online and offline consultations, and it is a positive development that the Council for the Rights of the Child will work closely with the Ombudsman for Children to monitor and promote children's rights. In recent years, the use of the internet and social media platforms has risen sharply. The risks were underestimated by parents, compounded by a lack of digital skills of parents, which may have contributed to the high rate of victims of cyberbullying in Romania. The lack of a legislative framework to protect children online and the current lack of integration of ICT components into education limit the promotion of online safety and awareness of online risks.

According to the author, among the prevention tools in Romania, the hotline operated by the Children's Helpline Association, a non-profit NGO, provides the only well-known free national helpline (*Telefonul Copilului*) for children and adolescents in Romania. *Romani Criss*, an NGO focused on Roma students, which, in cooperation with the Intercultural Institute, initiated measures to create a school mediator position in the Romanian public education system. In 1998 and 1999, school mediators were trained and employed in a pilot project to tackle early school leaving called the Second Chance Programme.

School mediation is one of the important measures designed to support Roma pupils, and it should be pointed out that, unfortunately, little information is available on the impact of this measure and the legal framework for the work of school mediators is rather vague, suggesting some uncertainty in Romanian legislation. School mediation can serve as an example for the codification and legislative activities of other countries, including Hungary, according to the author's point of view, who has been codifying for years.

There may also be liability if information promoted through the use of meta-links infringes the rights of third parties.

Outline of liability of service providers	
Monitoring body	(a) audit authority
Complaint handling	(a) measure of the audit authority
Sanctions	(a) fine ranging from 1,000 to 100,000 RON (b) other sanctions (criminal law)

Table 6. Outline of liability of service providers in Romania⁷⁶

⁷⁶ Source: author's own editing.

Law No. 365. of 2002 provides in general terms that service providers are subject to civil, criminal and administrative liability laws, and states that service providers are liable for information provided by them or on their behalf, but this liability cannot be regarded as absolute because it can only be enforced within certain limits.

Bibliography

- An overview on hate crime and hate speech Country profile: ROMANIA (2017)
- Athanasidou, K., Melegkovits, E., Andridatae, E. K., Magoulas, C., Tzavara, C. K., Richardson, C., Greydanus, D., Tsolia, M., Tsitsika, A. K. (2018) 'Cross-national aspects of cyberbullying victimization among 14–17-year-old adolescents across seven European countries', *BMC Public Health* volume 18, Article number: 800 <https://bmcpublikehealth.biomedcentral.com/articles/10.1186/s12889-018-5682-4>.
- Baldry, A., Blaya, C., Farrington, C., David P. (2018) 'Cyberbullying and Cybervictimization', in *International perspectives on cyberbullying prevalence, risk factors and interventions*, Michigan State University East Lansing, MI, USA
- Council of Europe (2019) *ECRI report on Romania*
- Chateau, C. (2016) *Cyberbullying among young people*. European Parliament, Brussels, <https://tinyurl.hu/5t9N>
- Dr. Casarosa, F. (2020) *Handbook on Techniques of Judicial Interaction in the Application of the EU Charter Freedom of expression and countering hate speech*
- Lefter, A., Sima, C. P. (2018) *Digital business in Romania: overview*. 2018
- Meza, R. (2016) 'Hate speech in the Romanian Online Media', *Journal of Media Research*, vol. 9 issue 3 (26)/2016
- Meza, R., Vincze, H. O., Mogoş, A. 'Targets of online hate speech in context. A Comparative Digital Social Science Analysis of Comments on Public Facebook Pages from Romania and Hungary.' in *Intersections. East European Journal of Society and Politics*
- Publications Office of the European Union (2018) Hate crime recording and data collection practice across the EU, FRA, Luxembourg
- Sorbán, K. (2019) 'Az internetes közvetítő szolgáltatók kettős szerepe a kiberbűncselekmények nyomozásában Felelősség és kötelezettségek', *In Medias Res*, 2019/1. 85–91.
- The Extreme Right and Roma and Sinti in Europe (2009) 'A New Phase in the Use of Hate Speech and Violence?', *Roma Rights Journal*, number 1
- Varga, A. (2019) *Román alkotmányjog*. Budapest–Köszvár: Forum Iuris
- Voinea, D. V. (2015) 'Media, Social Media and Freedom of Speech Protection in Romanian Legislation' *Creativity in Social Sciences*, Lund University

X. REGULATION OF DIGITAL OFFENCES IN THE 21ST CENTURY WITH SPECIAL REGARD TO THE CRIME OF DANGEROUS ELECTRONIC HARASSMENT IN SLOVAKIA

JÁNOS SZINEK

1. Regulatory aspects of hate speech

In the legal order of the Slovak Republic, the concept of hate speech (*nenávisťný prejav*) is not defined. However, EU instruments and the case law of the European Court of Human Rights (hereinafter referred to as the ECtHR) are of great help in defining this term. The jurisprudence of the ECtHR derives the concept of hate speech from Recommendation No. R (97) 20 of the Committee of Ministers of the Council of Europe of 30 October 1997 on hate speech,¹ as a *soft law* document. The Recommendation proposes a comprehensive approach combating hate speech, based on the seven principles detailed in its appendix, with a particular focus on hate speech disseminated through the media and its social, economic, political, cultural, and other causes.² Moreover, it defines hate speech as any expression of opinion that disseminates, promotes, justifies or incites racism, xenophobia, anti-Semitism or other forms of intolerance.³

1 Recommendation No. R (97) 20 of the Committee of Ministers to member states on 'hate speech'.

2 Boytha, 2008, pp. 10–20.

3 Kondorosi, 2015, p. 92.

In its decision, the Constitutional Court of the Slovak Republic (*Ústavný súd Slovenskej republiky*) stated⁴ that it agrees with the definition given above and describes the most common forms of hate speech. Accordingly, hate speech can be carried out by means of defamation, i.e., the public dissemination of statements, images, or videos with offensive or seriously defamatory content against a group of persons, and by means of incitement to hatred, i.e., the public dissemination of statements, images, videos or calls for hate and violence against certain groups of persons.⁵

Výborný is much more precise concerning the definition of hate speech. In his view, hate speech is speech that contains elements of hatred towards the group to which the speech is directed, or speech based on such hatred. In addition, hate speech is based on negative prejudices of the speaker against certain groups in society, which he insults, attacks, humiliates, calls for the restriction of their rights or acts of violence against them, or otherwise tramples on their human dignity. The words spoken affect not only the specific addressee, but the entire group to which the victim belongs.⁶

In general, a democratic society and the rule of law guarantee the right of every individual to express his or her views orally, in writing, in print, in images or otherwise, and to seek, receive and impart ideas and information freely, regardless of frontiers.⁷ It should be pointed out that freedom of expression and the right to free access to information is guaranteed⁸ by the highest source of law in the country, the Constitution of the Slovak Republic (*Ústava Slovenskej republiky*).⁹ The Slovak Constitution also provides for an explicit prohibition of censorship¹⁰ by declaring that freedom of expression and the right to seek and impart information may be restricted by law only where such restriction is necessary in a democratic society in order to protect the rights and freedoms of

4 See the decision of the Constitutional Court of the Slovak Republic No. PL ÚS 5/2017 of 9 January 2019.

5 Decision of the Constitutional Court of the Slovak Republic No. PL ÚS 5/2017 of 9 January 2019, p. 51.

6 *Výborný*, 2013, p. 18.

7 *Hulkó*, 2021, p. 246.

8 Article 26 of the Constitution of the Slovak Republic provides a constitutional framework for freedom of expression (*sloboda prejavu*) and right to information (*právo na informácie*). Article 26(1) of the Constitution of the Slovak Republic provides for freedom of expression and constitutional protection of the right to information in the territory of the Slovak Republic.

9 *Ústavný zákon č. 460/1992 Zb., Ústava Slovenskej republiky*. Hereinafter referred to as the Constitution of the Slovak Republic, or the Slovak Constitution.

10 Constitution of the Slovak Republic, Article 26(2) and (3).

others, or where justified on grounds of national security, public order, public health or public morality.¹¹

Freedom of expression guarantees citizens the right to express their thoughts and opinions. According to the Slovak constitutional approach, freedom of expression is a human right, and, moreover, a political right that ensures the dissemination of different political views and allows citizens to influence political developments in the state and participate in public events. It also allows for the holding of protest rallies and the uncensored dissemination of public information on public affairs, as well as the confrontation of citizens' ideas with the opinions of other citizens. Since an individual's freedom ends where another person's right to freedom begins, freedom of expression must not be abused to infringe another person's right. Negative information, even if untrue, can diminish a person's social credibility, and authority in the workplace, and disrupt social relationships. It is prohibited to report untrue information about events and to abuse freedom of expression to commit acts of violence.¹² In this context, extremism should also be highlighted as a legitimate limit to freedom of expression.¹³

Freedom of expression shall be enjoyed by natural and legal persons, and also by stateless persons and groups of persons without legal personality. The right to freedom of expression is constitutionally protected by Article 26 of the Slovak Constitution.^{14,15}

Although hate speech is not explicitly defined in the Slovak criminal law system, two forms of hate speech, defamation (*hanobenie*) and incitement to hatred

11 Constitution of the Slovak Republic, Article 26(4).

12 Hulkó, 2021, p. 246.

13 In this context, see the relevant provisions of the Slovak Criminal Code (paras. 421, 423 and 424).

14 Filip, 1998, p. 625.

15 Examining the level of statutory provisions, it can be seen that there are several legal acts that are more narrowly or broadly related to freedom of expression, such as the Act No. 40/1964 Coll., the Civil Code, as amended (*zákon č. 40/1964 Zb., Občiansky zákonník*); Act No. 300/2005 Coll., the Criminal Code, as amended (*zákon č. 300/2005 Z. z., Trestný zákon*); Act No. 22/2004 Coll. on Electronic Commerce, as amended (*zákon č. 22/2004 Z. z. o elektronickom obchode*); Act No. 211/2000 Coll. on Free Access to Information, as amended (*zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám*); Act No. 18/2018 Coll. on the Protection of Personal Data, as amended (*zákon č. 18/2018 Z. z. o ochrane osobných údajov*); Act No. 185/2015 Coll. on Copyright, as amended (*zákon č. 185/2015 Zb., Autorský zákon*); Act No. 308/2000 Coll. on Broadcasting and Retransmission, as amended (*zákon č. 308/2000 Zb. o vysielaní a retransmisii*); Act No. 167/2008 Coll. on Periodical Press Products and News Agencies, as amended (*zákon č. 167/2008 Zb. o periodickej tlači a agentúrnom spravodajstve*); Act No. 372/1990 Coll. on Administrative Offences, as amended (*zákon č. 372/1990 Zb. o priestupkoch*); Act No. 351/2011 Coll. on Electronic Communications, as amended (*zákon č. 351/2011 Z. z. o elektronických komunikáciách*).

(*podnecovanie k nenávisti*), are declared as criminal offences.¹⁶ These are covered by the sections of the Criminal Code on defamation of nationality, race and beliefs (*hanobenie národa, rasy a presvedčenia*) and incitement to national, racial and ethnic hatred (*podnecovanie k národnostnej, rasovej a etnickej nenávisti*).¹⁷

Freedom of expression and hate speech are often seen to ‘collide’. It is very difficult to find the right balance between the two categories. It is the duty of the law to determine in a reasonable and fair way where freedom of expression ends and where a statement becomes defamatory or hate speech.

Freedom of expression is of paramount importance in a society because it makes social debate more likely to reveal the truth and eliminate political error. However, this process can be fraught with emotion, criticism, and even insults and mockery, which is necessary if society is to move forward by confronting criticism. Therefore, freedom of expression, by its very nature, always entails the risk of conflict between individuals, whether in private or in public communication. On this basis, freedom of expression should be understood as a so-called conflictual freedom: a freedom that in most cases entails confrontation and potential sources of conflict.¹⁸

However, the unclear definition of hate speech and the lack of a uniform definition creates significant problems in drawing the line and also creates a perceived legal uncertainty. This is both apparent and perceptible in EU and national legislation.

2. Cyberbullying in Slovakia

As today’s society is often described as an information society, the 21st century is often referred to as the digital age. Communication and information technologies are not only pervasive, but they are also an integral part of society. All age groups of the population, from children to young people, from the productive population to the elderly, fit into this framework. It also paints a picture of the intertwining of information technologies and population, of how these technologies are integral not only to the modern age but also to different aspects of the lives of individuals, groups and populations.¹⁹

¹⁶ Erdősová, 2019, pp. 448–449.

¹⁷ Act No. 300/2005 Coll., as amended (*Zákon č. 300/2005 Z. z., Trestný zákon*). Hereinafter referred to as the Slovak Criminal Code or Criminal Code.

¹⁸ For more information, see Lalík, 2016, pp. 1054–1066.

¹⁹ Kurucová, 2018, p. 37.

However, with the evolution of modern technology, a new problem has emerged in our society that the older generation is not yet aware of. The cyber-space environment is evolving and constantly developing, and with it a new form of 'danger'. In our case, we are talking about a form of bullying that is directly dependent on these technologies. We call this form of intimidation cyber intimidation.²⁰

In relation to freedom of expression, the Slovak Constitution declares that everyone has the right to freedom of speech and information, the right to express his or her opinion orally, in writing, in the press, in images or in any other form, and the right to seek, receive and impart ideas and information freely, regardless of frontiers.²¹ In contrast to the Hungarian legislation,²² the Slovak Constitution contains only enabling provisions on the exercise of freedom of expression, but no restrictive or prohibitive provisions.

Looking at the statutory level, it can be seen that the Slovak Criminal Code is the most relevant legislation for the research topic.²³ Under the Slovak Criminal Code, an offence is a qualified case if it is committed with a 'special motive'. Such a special motive could be, for example, when the offence is committed out of hatred of a group or individual on the basis of race, nationality, nationality or ethnic origin, race, colour, sex, sexual orientation, political or religious beliefs.²⁴

The list of substantive offences with more serious penalties for specific motives (direct intention) includes murder, assault, trafficking in human beings, threats, violence against a specific group of citizens or against a person, violation of personal liberty, kidnapping, robbery, extortion, restriction of religious freedom, violation of privacy of correspondence, theft, abuse of power, sexual violence, assault and rape.²⁵

20 Valihorová és Surovcová, 2018, p. 42.

21 Constitution of the Slovak Republic, Article 26(1) and (2).

22 Article IX (5) of the Hungarian constitution: "*The exercise of freedom of expression may not be directed against the dignity of the Hungarian nation, national, ethnic, racial or religious communities. Persons belonging to such communities shall have the right, in accordance with the law, to assert their claims before the courts against the expression of opinions that offend the community and violate their human dignity.*"

23 In addition to the Slovak Criminal Code, the Criminal Procedure Code [Act No. 301/2005 Coll., as amended (*Zákon č. 301/2005 Z. z., Trestný poriadok*)] is also an important source of law.

24 Criminal Code, para. 140 point e).

25 For further see the publication of the European Union Agency for Fundamental Rights named *Hate crime recording and data collection practice across the EU* c. page 79, online available at https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-hate-crime-recording_en.pdf

In addition, the Criminal Code penalises the creation, support or promotion of a group, movement or ideology which aims to suppress fundamental rights and freedoms, or which incites racial, ethnic, national or religious hatred or hatred against another group or person. In addition, the law prohibits the promotion of any group, movement or ideology which has in the past aimed at the suppression of fundamental rights and freedoms. This provision is supplemented by the Criminal Code, paras. 422 and 422a)–422c), which prohibit public manifestations of support for these groups, movements or ideologies, as well as the production, distribution and possession of extremist material (e.g., publications and leaflets).²⁶

In addition, the Criminal Code defines as a criminal offence the public defamation of any nation, its language, any racial or ethnic group, or of any person or group of persons on the basis of any race, nation, nationality, colour, ethnic group, political opinion, religion or lack thereof.²⁷

Finally, para. 424 of the Criminal Code is also remarkable, which defines the offence of incitement to national, racial and moral hatred. In conclusion, the concept of cyberbullying has not been defined in the Slovak Republic.²⁸ The Criminal Code does not regulate neither bullying (*šikanovanie*) nor cyberbullying (*kyberšikanovanie*), nor does it define these categories.²⁹

On 8 June 2021, the Head of State Čaputová signed a proposal to amend the law,^{30, 31} effective from 1 July 2021, which, among others, introduces a new offence of dangerous electronic harassment³² (*nebezpečné elektronické obťažovanie*) into the Slovak Criminal Code, which essentially covers the most serious cases of cyberbullying.³³

It should be stressed that dangerous electronic harassment as a criminal offence was introduced into the Slovak legal system essentially without any precedent, as electronic harassment *per se* was not a criminal offence before the entry into force of the provision in question.³⁴

26 Criminal Code, paras. 422 and 422a)–422c).

27 See: Criminal Code, para. 423. In this context, see also: European Union Agency for Fundamental Rights: *Hate crime recording and data collection practice across the EU* page 79. Online available: https://fra.europa.eu/sites/default/files/fra_uploads/fra-2018-hate-crime-recording_en.pdf

28 Hulkó, 2021, p. 302.

29 Parti, 2016, p. 117.

30 The Slovak Parliament approved the proposed amendment on 27 May 2021.

31 The full text of the proposal in Slovak can be found at: <https://www.najpravo.sk/clanky/prezidentka-podpisala-zakon-ktorym-sa-doplna-trestny-zakon.html>

32 For more on this topic, see Šmigová, 2023, pp. 165–197.

33 See para. 360b of the Criminal Code.

34 Bielik, 2022.

Under the new regulation, a person who intentionally humiliates, intimidates, unlawfully acts on behalf of another person, or intentionally harasses another person in a persistent manner through an electronic communications service provider, computer network or system, may be sentenced to up to three years imprisonment. It is also a criminal offence to unlawfully disclose or make available to another person a visual, audio or visual and audio recording of a personal speech obtained with the consent of the person concerned, provided that the recording is capable of endangering the human dignity or otherwise seriously prejudicing the rights of the person concerned. If the offender commits the offence with a specific motive (direct intention) or commits the offence against a protected person, the perpetrator may be sentenced of up to one to four years. If the offender causes substantial damage by committing the offence, or commits the offence with the intention of obtaining a substantial benefit, or has been convicted of such an offence one or more times in the previous 24 months, he shall be punished with imprisonment for a term of between two and six years.³⁵

The definition of dangerous electronic harassment includes the most serious and dangerous cases of cyberbullying, i.e., crimes that are intended to cause long-term, intentional harm to the victim's quality of life. The publication of personal (visual and/or audio) recordings obtained by the offender with the consent of the victim is only punishable if they are recordings of personal expressions that are capable of causing serious harm to the victim. This latter specification is intended to avoid disproportionate punishment.³⁶

In conclusion, regulating dangerous electronic harassment is very timely, as cyberbullying is a modern, widespread phenomenon that causes serious problems in the online space.³⁷

In Slovakia, the following offences are the most frequent in the context of cyberbullying: dangerous threat (*nebezpečné vyhrážanie*),³⁸ dangerous persecution (*nebezpečné prenasledovanie*),³⁹ production and distribution of child pornog-

³⁵ Criminal Code, para. 360b(1)–(4).

³⁶ Ružarovský, 2021.

³⁷ Vanc, 2021.

³⁸ Criminal Code, para. 360.

³⁹ Prior to the entry into force of the amendment in this amendment, this provision was the provision that covered cyberbullying the most. See in particular Article 360a(1) point c) of the Criminal Code:

“(1) Whoever regularly or persistently harasses another person or, with respect to him, his relative, in a manner likely to cause fear or disruption of his daily life, by:

(a) threatening to commit an act prejudicial to the health or integrity of that person or, with respect to that person, of a relative,

(b) seeking or following his or her proximity,

raphy (*výroba detskej pornografie, rozširovanie detskej pornografie*),⁴⁰ possession of pornographic recordings of children and participation in child pornographic performances (*prechovávanie detskej pornografie a účasť na detskom pornografickom predstavení*),⁴¹ endangering the moral development (*ohrozovanie mravnosti*),⁴² endangering the moral education of young people (*ohrozovanie mravnej výchovy mládeže*),⁴³ extortion (*vydieranie*),⁴⁴ coercion (*nátlak*),⁴⁵ sexual abuse (*sexuálne zneužívanie*)⁴⁶ and defamation (*ohováranie*).^{47,48}

2.1. Bullying at schools

A general examination of the legislation in this area,⁴⁹ as well as the government decrees (*nariadenia vlády*), regulations (*vyhlášky*) and directives (*smernice*) issued by individual ministries, shows that they do not explicitly address bullying in schools. Under Act No. 596/2003 Coll. on the State Administration of Education and School Self-Government, as amended⁵⁰ the Ministry directs the activities of the State Administration of Education by developing concepts under the above-mentioned Act and by issuing generally binding legislation, directives, instructions and by standardising their application, and monitors their implementation.⁵¹ It should be noted, however, that directives, ministerial decrees

(c) by contacting him or her with the assistance of a third person, by electronic means of communication, in writing or otherwise, against his or her will,

(d) misuses his or her personal data for the purpose of establishing a personal or other relationship; or

(e) otherwise interferes with his or her daily activities, shall be punishable by a maximum term of imprisonment of up to one year.

(2) The punishment shall be imprisonment for a term of six months to three years if the act referred to in paragraph 1

a) to the detriment of a protected person,

b) in a more serious manner,

c) with special motive, or

(d) committed in a public place.”

40 Criminal Code, paras. 368 and 369.

41 Criminal Code, para. 370.

42 Criminal Code, paras. 371 and 372.

43 Criminal Code, para. 211.

44 Criminal Code, para. 211.

45 Criminal Code, para. 192.

46 Criminal Code, paras. 201, 201a and 201b.

47 Criminal Code, para. 373.

48 Izakovič, 2021.

49 Hrášková, 2015.

50 Zákon č. 596/2003 Z. z. o štátnej správe v školstve a školskej samospráve.

51 Act No. 596/2003 Coll. on the State Administration of Education and School Local Authorities, as amended, para. 14(1).

and methodological instructions, as internal professional documents, are not published in the Collection of Laws of the Slovak Republic (*Zbierka zákonov Slovenskej republiky*) and are therefore not considered to be statutory legislation in this sense, but are binding on schools and educational institutions and their implementation can be monitored.⁵²

Among those mentioned above, Directive 36/2018/EU on the Prevention and Treatment of Bullying of Children and Pupils in Schools and Educational Establishments should be highlighted,⁵³ which repealed Methodological guidance No. 7/2006-R of 28 March 2006 regarding the prevention and dealing with bullying of students at schools and school facilities.⁵⁴ The Directive, which is still in force, defines the basic signs, forms and manifestations of bullying of children and pupils, as well as the possibilities for preventive measures and methods of dealing with bullying of pupils.⁵⁵

It should also be noted that schools currently have a number of relevant methodological materials and manuals, as well as a few websites that take a comprehensive and interactive approach to bullying and cyberbullying in schools.⁵⁶ Close cooperation between schools and educational counselling and prevention services is also an important part of tackling these dangerous social phenomena.⁵⁷

On the basis of the requirements of the Ministry of Education, Science, Research and Sport of the Slovak Republic (*Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky*)⁵⁸ at the Department of Prevention and Youth Research of the Scientific and Technical Information Centre of the Slovak Republic [*Centrum vedecko-technických informácií Slovenskej republiky (CVTI SR), Oddelenie prevencie a výskumov v oblasti mládeže*] has been mapping the problems of bullying in schools for a long time. Through data collection, the research focuses on the following areas of the problem under study: prevalence and manifestations, methods of treatment, cooperation with the different actors, and organisation of prevention activities/programmes. Among the

⁵² Havrila, 2021.

⁵³ *Smernica č. 36/2018 k prevencii a riešeniu šikanovania detí a žiakov v školách a školských zariadeniach*

⁵⁴ *Metodické usmernenie č. 7/2006-R z 28. marca 2006 k prevencii a riešeniu šikanovania žiakov v školách a školských zariadeniach*. Available at: <https://www.minedu.sk/data/att/16073.pdf>

⁵⁵ For more on this subject, see the Directive 36/2018/EU on the Prevention and Treatment of Bullying of Children and Students in Schools and Educational Establishments.

⁵⁶ See, for example, <https://www.odpisemeti.sk/> (translated as www.wewillwriteback.sk). and also <https://www.kybersikanovanie.sk/index.php/slovník>

⁵⁷ For further, see Hrašková, 2015.

⁵⁸ Hereinafter referred to as the Ministry of Education.

directly managed and involved organisations of the Ministry of Education, Science, Research and Sports of the Slovak Republic, the Research Institute of Child Psychology and Pathopsychology (*Výskumný ústav detskej psychológie a patopsychológie*), which carries out a number of professional and methodological activities, should be mentioned.⁵⁹

2.2. *Bullying at work*

Neither international, nor EU, but even national legislation not defines precisely the legal definition of bullying at work. Research and various sources on the subject are based on different definitions developed by other social sciences, such as bullying and its forms (mobbing, bossing). The lack of a legal definition of bullying also implies a lack of a legal definition of cyberbullying.⁶⁰

Anti-discrimination legislation includes the concept of bullying as defined in Council Directive 2000/78/EC,⁶¹ which sets out a general framework for equal treatment in employment and occupation.

In Slovakia, the Labour Code⁶² states among its basic principles that ‘natural persons have the right to free choice of employment and occupation, fair and satisfactory working conditions and protection against arbitrary dismissal in accordance with the principle of equal treatment in the field of labour law, as laid down in the special Act on the Principle of Equal Treatment in Certain Areas and the Act on Protection against Discrimination (Anti-Discrimination Act), as amended and supplemented several times.’⁶³ The Labour Code also lays down as a fundamental principle the rule prohibiting the abuse of rights and obligations arising from the employment relationship to the detriment of the other party to the employment relationship and of the group of workers.⁶⁴ In cases where the legal framework is exceeded by the actions of either the employee or the employer to the extent that violence (mainly psychological, but physical violence cannot be excluded) is used, we are talking about bullying and its various forms.⁶⁵

⁵⁹ Havrila, 2021.

⁶⁰ Minčíčová, p. 130.

⁶¹ Council Directive 2000/78/EC establishing a general framework for equal treatment in employment and occupation. See: <https://eur-lex.europa.eu/legal-content/HU/TXT/?uri=CELEX%3A32000L0078>

⁶² Act No. 311/2001 Coll., as amended (*Zákon č. 311/2001 Z. z., Zákonník práce*)

⁶³ Labour Code, Principles, para. 1, 1st sentence.

⁶⁴ Labour Code, Principles, para. 1, 2nd sentence.

⁶⁵ Beznosková, 2020.

Examining the practice of bullying in the workplace, we found a number of relevant cases.⁶⁶ One of the facts can be summarised simply as follows: the employee was working in a job that the employer had classified in its internal rules of employment as a position for which an appointment by the employer was required.⁶⁷ The employer removed the employee from his position and subsequently dismissed the employee for failure to comply with the work requirement under para. 63(1) point d) and (2) of the Labour Code. The issue of discrimination was also examined during the proceedings. As the issue of bullying is relevant for the purpose of this chapter, the question of the nullity of the termination of employment and the discriminatory conduct of the employer will not be analysed separately. According to the Court's judgment, bullying shall be distinguished from discrimination. According to the judgment, the basis for discrimination is defined by the anti-discrimination law. The purpose of the Anti-Discrimination Act is to enforce the principle of equal treatment and to regulate the means of legal protection in the event of a breach of this principle. According to the Anti-Discrimination Act, compliance with the principle of equal treatment also means compliance with the prohibition of discrimination on the grounds set out in the Act. These grounds may be: sex, religion or belief, race, nationality, ethnic or national affinity, disability, age, sexual orientation, marital status, colour, language, political or other opinions, national or social origin, property, birth, or other status.⁶⁸

In general, in labour law, discrimination is defined as any discrimination, exclusion, or favouring based on discriminatory characteristics and intended to jeopardise or completely prevent equal opportunities or equal treatment of workers within the employment relationship. According to the Labour Code, discrimination consists primarily in the fact that the discriminated employee is the bearer of a certain characteristic. If a worker is persecuted

66 Judgment of the District Court of Banská Bystrica, case no.16 CoPr 11/2012 (*Rozsudok Krajského súdu v Banskej Bystrici sp. zn. 16 CoPr 11/2012*). Bullying is not explicitly mentioned in the Labour Code. By analogy, bullying can be considered a specific type of abuse of rights. The prohibition of abuse of rights is enshrined in the Labour Code in para. 2 of the Fundamental Principles. This formulation contains a legal prohibition and a legal injunction, which are the limits to the exercise of rights, the exercise of rights and the fulfilment of obligations. The 'prohibition of abuse of rights' in para. 2 of the Fundamental Principles of the Labour Code constitutes a legal norm, the violation of which by those entitled to it constitutes an unlawful act. The specificity of such an unlawful act is that it does not result from the breach of a legal obligation, but occurs in the exercise of a right in a manner prohibited by law.

67 Labour Code, para. 42(2).

68 Beznosková, 2022.

for other reasons, this does not constitute discrimination, but may amount to bullying.⁶⁹

The above-mentioned decision of the court makes a distinction between bullying and discrimination. The judgment states that bullying is not explicitly provided for in the Labour Code, and therefore, by analogy, bullying can be considered a specific type of abuse of rights. Simply put, the judgment was about bullying by the employer, i.e., bossing. Both the employer and the manager have both the right and the duty to control subordinate employees, to give them instructions, and to require them to perform their work in accordance with the mandatory conditions of employment laid down in the employment legislation. A simplified interpretation of this relationship is that the employer and the manager exercise certain rights and obligations over the subordinate workers and that within this relationship there may be an abuse of rights.⁷⁰

3. Legislation on prevention and case law

Cybersecurity has become an increasingly popular topic in Slovakia over the past few years, as evidenced by the fact that the Government of the Slovak Republic (*Vláda Slovenskej republiky*)⁷¹ has drafted a new cybersecurity law in the country during this period, which amended the Common and Uniform Practices for Cyber Defence.⁷² The preparations were complex, involving not only experts from the public administration but also the academic community, civil society, and many other experts. In addition to the Cybersecurity Act, Slovakia has already had a National Strategy for Information Security (*Národná stratégia kybernetickej bezpečnosti*) since 2008, and a technical document, the Cybersecurity Concept 2015–2020, prepared by the National Agency for Network and Electronic Services (*Národná agentúra pre sieťové a elektronické služby*) and the National Security Authority (*Národný bezpečnostný úrad*) and adopted by the Government in June 2015. The National Cybersecurity Strategy 2021–2025⁷³ was approved by the Slovak Government on 7 January 2021 by Decision No. 5/2021. It was the first strategy document

⁶⁹ Beznosková, 2022.

⁷⁰ Švec, 2019, pp. 12–17.

⁷¹ Hereinafter referred to as the Slovak government or government.

⁷² Act No. 69/2018 Coll., as amended (*Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti*).

⁷³ *Koncepcia kybernetickej bezpečnosti Slovenskej republiky na roky 2015–2020*

that comprehensively defined the Slovak Republic's strategic approach to cybersecurity.⁷⁴

The issue of child protection in the digital space, and the evolution and nature of threats, is a very dynamic and rapidly changing phenomenon. Therefore, a coordinated, coherent and transparent response, as well as adequate political and institutional support, is needed to address the situation. For the period 2020–2025, the Slovak Government has developed a National Strategy for the Protection of Children in the Digital Space (National Strategy).⁷⁵ Given that this is a rapidly evolving area, the National Concept for the Protection of Children in the Digital Space proposes measures for each specific objective, which will be reflected in a short-term action plan. In addition to the concept, three action plans will be prepared for a two-year period, taking into account the current situation and evolution of the protection of children in the digital space and their vulnerability.

The National Strategy lists the actors involved in institutional and policy support for the protection of children in the digital space, but does not clarify their responsibilities and roles.⁷⁶

In Slovakia, there are a number of non-profit organisations working on cyberbullying issues and running various websites. For example, the website www.pomoc.sk (translated as www.help.sk)⁷⁷ provides useful advice and assistance to those concerned about aggressive, violent and abusive behaviour, misuse of personal data, communication on social networks and inappropriate content.

74 Available online on the official website of the Slovak National Security Office: https://www.nbu.gov.sk/wp-content/uploads/kyberneticka-bezpecnost/Strategia_kybernetickej-bezpecnosti_2021.pdf

75 National concept for the protection of children in digital space. Online available: https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf

76 The organisations involved in the technical work were the following: Office of the Government of the Slovak Republic; Office of the Deputy Prime Minister for Investments and Informatization; Ministry of the Interior of the Slovak Republic – Government Council for Crime Prevention; Ministry of Education, Science, Research and Sports of the Slovak Republic; Ministry of Culture of the Slovak Republic; Ministry of Justice of the Slovak Republic; Ministry of Labour, Social Affairs and Family of the Slovak Republic; Ministry of Health of the Slovak Republic; the Ministry of Finance of the Slovak Republic; the Office of the Commissioner for Children's Rights; the Office for Personal Data Protection of the Slovak Republic; the Office for the Protection of Industrial Property of the Slovak Republic; the Police of the Slovak Republic, the Prosecutor's Office, the Courts; universities, the Slovak Academy of Sciences, the Audiovisual Fund, registered churches and religious associations, NGOs, other representatives of civil society, psychologists, municipalities, schools, educational institutions, health care providers and other organisations.

77 The page is available at <http://www.pomoc.sk>

People in need of help and those affected can contact the organisation 24 hours a day by e-mail (chat) or telephone at potrebujem@pomoc.sk (translated as ineed@help.sk). Also worth mentioning is the website www.stopline.sk, which allows you to report inappropriate or illegal content and activities. Reporting is completely anonymous and can be done by filling in an online form.⁷⁸

The project, operated by the eSlovensko civil association⁷⁹ – *Zodpovedne.sk* (translated as *Responsibly.sk*)⁸⁰ – aims to raise awareness, educate people about responsible use of the internet, mobile communications and new technologies, and prevent related crimes. The organisation's activities focus on all forms of aggression in cyberspace, including cyberbullying. In addition, other projects of this civil association, such as *Nehejtuj* (translated as *Do not hate*)⁸¹ and *Ovce.sk* (translated as *Sheep.sk*),⁸² which highlight the pitfalls and harmful and dangerous consequences of cyberspace activities in an age-appropriate way for the target audience, should also be mentioned. They also include *Kyberšikanovanie – narodení pre výhru* (translated as *Cyberbullying – born to win*), *Rythmus – sídliskový sen* (translated as *Rhythm – a dream in a housing estate*) and *No Problemos*, which focus on preventing cyberbullying and online exclusion.⁸³

Within this chapter, we also need to address the question of whether national law provides for any form of blocking of access to hate speech or cyberbullying in online spaces and, if so, what are the limits of this measure? In the course of our research, we found that neither the Criminal Code nor the Criminal Procedure Code⁸⁴ explicitly mention the terms 'inaccessibility' or 'electronic data'. In contrast, a provision of the Criminal Procedure Code explicitly provides for the retention, release and withdrawal of computer data. In cases where the retention of electronically stored computer data, including operational data stored by means of a computer system, is necessary for the evidentiary procedure, the prosecutor may, before the commencement of the procedure or during the

⁷⁸ See the websites mentioned.

⁷⁹ For a definition of civil association, see para. 2(1) of Act No. 83/1990 Coll., on Association of Citizens, as amended (*Zákon č. 83/1990 Z. z. o združovaní občanov*): "Citizens may establish and join associations, associations, federations, movements and other civil associations, as well as trade unions (hereinafter referred to as 'associations')."

⁸⁰ The project is available not only in Slovak, but also in English by following the link <https://www.zodpovedne.sk/index.php/en/>

⁸¹ The project for secondary school students deals with intolerance.

⁸² The online project Sheeplive.eu/*Ovce.sk* is aimed primarily at pre-school children, where the website aims to raise awareness of the pitfalls of online communication through short animated stories.

⁸³ Hollá et al., 2017, p. 44.

⁸⁴ *Zákon č. 301/2005 Z. z., Trestný poriadok*.

preparatory procedure, issue a factual order requiring the suspect to: preserve and maintain the integrity of such data, allow copies of such data to be made and preserved, prevent access to such data, remove such data from the computer system, disclose such data for evidentiary purposes without delay.⁸⁵

However, this legal provision implies the complete inaccessibility of the data, since the order under paragraph 1(a) to (c) of the above-mentioned provision must specify the period of retention of the data, which may not exceed 90 days. If justified, a new order may be issued for a further period of 90 days.⁸⁶

The fact that cyberbullying is an increasingly serious threat to society is confirmed by a survey by the insurance company Uniqua.⁸⁷ It shows that around 90% of respondents do not know how to protect themselves in such cases. The insurance company's cyber insurance package offers a solution. According to the call, if someone is a victim of bullying on the internet, they simply need to call Uniqua's helpline and the insurer will ensure that such information is removed or deleted from the internet. The victim is also entitled to legal representation and reimbursement of related costs. In such a case, the insurer will ensure that the offensive or defamatory messages are deleted, block the profile of the attacker and provide other legal and IT assistance. Cyber insurance not only covers cyberbullying, but also provides comprehensive protection against damage to an online person's reputation. It also covers the theft and publication of photographs taken from a mobile phone, if the theft is due to misuse of the identity of the insured or if the publication damages the online reputation of the customer. Defamation, insulting or unlawful disclosure of private information is considered a breach of online reputation.⁸⁸

4. Responsibilities of service providers and institutions

A major problem in the country remains that Slovak legislation does not clearly define how to deal with and prosecute offences committed in the digital space. In the context of cybercrime, the prosecution deals mainly with cases of child pornography, harassment, sexual abuse and similar offences, as domestic

⁸⁵ Criminal Procedure Code, para. 91(1).

⁸⁶ Criminal Procedure Code, para. 91(2).

⁸⁷ For further see: <https://www.uniqua.sk/o-nas/aktuality/urazy-pocas-prestavky-kradeze-kybersikana-kto-nesie-zodpovednost-za-skody-ktore-stanu-ziakom-skole.html>

⁸⁸ For further see: <https://www.finreport.sk/banky-a-poistovne/z-kybersikany-sa-stal-trestny-cin-ochranu-obetiam-poskytuje-nielen-zakon-ale-aj-kyberpoistenie/>

legislation does not recognise other forms of online abuse and exploitation of children, such as sexting or hate speech.⁸⁹

Currently, there is no legislation in Slovakia that imposes specific obligations on internet service providers and website (social networking) operators, but there are some obligations under certain laws. One example is the obligation of prevention, which is laid down in the Civil Code. It states that “*everyone has the duty to act in such a way as to prevent damage to health, property, nature and the environment.*”⁹⁰ This applies not only to those who suffer damage but also to those who cause it. It can also apply to the operator of a social network if it is aware that its network is being widely used for cyberbullying, yet does nothing to prevent it.

The legal regime for internet broadcasters is much lighter than that for traditional broadcasters between licences. The legislation in question⁹¹ does not regulate all content on the internet, but only covers content broadcast over the internet and content that is part of an on-demand audiovisual media service.⁹²

In Slovakia, most website operators do not substantially restrict children’s access to pornographic content. Content intended exclusively for over 18 years is unrestricted and can be accessed by simply clicking on the OK button, which does not even require reading the warning text (which usually contains information that the pages to be opened contain pornographic content and a warning that such content is not accessible to under 18 years of age). This also applies to specific cases of sexting, where the ‘perpetrator’ is very often the victim, and thus punished by the laws originally designed to protect the victim.⁹³

In addition, content providers in Slovakia are making increasing efforts to combat discriminatory and other illegal or harmful content through self-regulation, in particular in the form of codes of conduct. Some websites also display

89 National Concept for the Protection of Children in the Digital Space (*Národná koncepcia ochrany detí v digitálnom priestore*), p. 4. Available online: https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf

90 Slovak Civil Code, para. 415.

91 Act No. 308/2000 Coll. on Broadcasting and Retransmission, as amended (*Zákon č. 308/2000 Z. z. o vysielaní a retransmisii a o zmene zákona č. 195/2000 Z. z. o telekomunikáciách v znení neskorších predpisov*).

92 For internet broadcasting to be covered by the regulation, it must fully comply with all the characteristics of broadcasting services as defined in para. 3(1) of Act No. 220/2007 Coll. on Digital Broadcasting, as amended.

93 National Concept for the Protection of Children in the Digital Space (*Národná koncepcia ochrany detí v digitálnom priestore*), p. 7. Available online: https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf

a label for each code of conduct, indicating that the site complies with the code of conduct. In addition, content providers are working to develop and facilitate access to child-friendly content, for example through the creation of special websites and search engines for children. It remains a concern that progress in this area is still significantly weak. In the future, existing measures against illegal or harmful content for children will need to be continuously monitored to ensure their effectiveness.⁹⁴

The Slovak legal system does not specifically regulate social media. The only legislation in force that has some direct relevance to the liability of community media is Act No. 22/2004 Coll. on Electronic Commerce, as amended, which was adopted to transpose the provisions of the Directive on electronic commerce into national law. The law is not specifically aimed at regulating social media platforms, but it also applies to these platforms.⁹⁵

Slovak legislation does not define the concepts of illegality and infringement, neither for e-services nor for social media. As a general rule, the removal of infringing content and the infringement suffered online may lead the victim to take legal action. In the area of personal data protection and copyright protection, there is a sectoral public administration supervisory body, and therefore intervention is possible under sectoral legislation. The Slovak legislation does not distinguish between infringements committed online and offline and therefore the nature of the medium is not relevant for the availability of legal remedies.⁹⁶

For these reasons, it would be very difficult to hold the largest group of service providers liable for the data and information they store or transmit. The exceptions to this are news portals, online radio and television channels, because they produce the information and news themselves or have significant influence over it. Such providers moderate their own forums and remove posts that violate rights or public morals, following the ECtHR' judgment in *Delfi AS v. Estonia* of 10 October 2013.⁹⁷

Service providers are under no obligation to monitor users' content, and the regulation explicitly prohibits service providers from pre-filtering users' data

94 National Concept for the Protection of Children in the Digital Space (*Národná koncepcia ochrany detí v digitálnom priestore*), p. 18. available online: https://detstvobeznasilia.gov.sk/web_data/content/upload/subsubsub/2/narodna-koncepcia-ochrany-deti-v-digitalnom-priestore-1.pdf

95 Hulkó, 2021, p. 250.

96 Ibid., p. 251.

97 The case *Delfi AS v Estonia* can be accessed by clicking on the following link: <https://hudoc.echr.coe.int/eng#%7B%22documentcollectionid%22:%5B%22GRANDCHAMBER%22,%22CHAMBER%22%5D,%22itemid%22:%5B%22001-126635%22%5D%7D>

without their consent. If the service provider becomes aware of the illegality of such information (for example, through the notice and take-down procedure), it is obliged to remove it or prevent access to it as soon as possible. Searching for user information is therefore generally excluded, and the provider is not obliged to actively search for infringing content. Currently, there is no uniform legal or academic position in Slovakia on the interference of social media platforms with unlawful user content. The literature cites the court case *Stacho v. Klub Strážov*, in which a website was challenged for a post (comment) that violated the human dignity of a specific person.⁹⁸

4.1. Responsibilities of educational institutions

The school, together with the family, has a decisive and determining influence on the development of the young generation. In addition, the role of the school is gradually shifting from its current educational and training function to a social, emotional and preventive role against the undesirable influences of society.⁹⁹ The preventive function of schools in the school environment, in extra-curricular activities and in leisure time activities has also become an often-debated topic. What is more, school as an institution provides pupils with a place for education and training that should lead to positive changes in the development of the pupil.¹⁰⁰

However, today's schools have to deal more and more intensively with pupils' learning difficulties, which are on the rise. Aggressive behaviour has consequences for pupils, especially in the areas of social relationships, communication between pupils, interaction, cooperation, trust, participation in problem solving, belonging and discipline. At the same time, the impact of aggressive behaviour in school is to reduce the emotionality of the pupils, to create a collective lack of socially accepted values and to create a fear of the school environment. Fear arises in situations where the satisfaction of certain needs, especially the need for safety and security, is threatened, either in reality or in the imagination.¹⁰¹

The learning environment, by which we mean primarily the school environment, provides an opportunity to develop the learner's resilience. For students who have a less stimulating and more stressful than average home environment, this school environment is very important and the school should provide them

⁹⁸ Hulkó, 2021, p. 252.

⁹⁹ Hollá et al., 2017, p. 49.

¹⁰⁰ Ibid.

¹⁰¹ Vágnerová, 1994, p. 273.

with a sense of achievement, which is important for the student's self-esteem. The compensatory function of the school environment is important for all learners. It is particularly valuable for pupils who come from a non-affirming family background. In this case, the school environment is of particular importance to the pupil, who needs to feel a sense of belonging, a sense of belonging to a group and a sense of achievement. As part of the extra-curricular activities in which children participate, activities that help them to make decisions are important. They teach children the real responsibility that comes with resilience and contribute to their sense of identity.¹⁰²

Schools and educational establishments play an important role in prevention systems at regional and local level, as the majority of young people attending school become the direct target of prevention measures. Skácelová defines the practical role of schools in prevention activities as follows: children's first serious behavioural problems, which usually require specialised care, are most often encountered in primary school; the Ministry of Education has an extensive network of counselling institutions and the counselling services they provide; children usually show the first signs of problem behaviour long before they come into the care of the social assistance services of the Department of Social Work; the social and health services come to the rescue when intervention is needed in the family and usually when comprehensive preventive activities initiated by the school need to be implemented; school and school facilities are often the only environment in which peer influence can be systematically corrected, especially in the case of disorganised individuals.¹⁰³

Effective prevention in the school environment requires first and foremost a safe school atmosphere.

4.2. Responsibility of the employer

Traditional cases of bullying show that if an employee suffers damage as a result of abusive behaviour at work, he or she can claim compensation through the institution of general employer's liability.¹⁰⁴

According to the Slovak Labour Code,¹⁰⁵ the employer is liable to the employee for damages caused to the employee by a breach of statutory obligations or intentional conduct contrary to good morals in the course of or directly related to the performance of his/her duties. It is irrelevant in law whether the damage was

¹⁰² Kardos, 2007, p. 576.

¹⁰³ Skácelová, 2003, p. 329.

¹⁰⁴ Labour Code, para. 192.

¹⁰⁵ Labour Code, para. 192(1).

caused by another employee, by an employee acting on behalf of the employer or by a third party. It follows from the above that an employee who suffers damage caused by an act of a person outside the employment relationship is also entitled to claim compensation from the employer. In view of the above-mentioned specificities of cyberbullying, the possibility to claim compensation is limited by the presumption that the damage occurred in the course of or in direct connection with the performance of work duties within the meaning of the Labour Code.¹⁰⁶ If, even in these cases, the law were to include a presumption of liability in relation to the performance of the work tasks, it would be possible for an employee abused by a third party to bring a claim for compensation.¹⁰⁷ The employer's general liability for damages is supplemented by a third cause of action, which is no longer linked to the presumption that the damage occurred in the course of or in direct connection with the performance of the work. The employer is liable to the employee for damage caused by the breach of statutory obligations by employees acting on behalf of the employer in the performance of their employer's duties.

Given that suicide is mentioned in the literature as one of the possible consequences of cyberbullying, it is also worth considering whether 'survivors' can claim compensation under the employer's liability for an accident at work. No relevant judgments were found in Slovakia on this point, but – regularly cited in the Slovak literature – the Constitutional Court of the Czech Republic (*Ústavní soud České republiky*) handed down a decision in a case of suicide of an employee, which the plaintiff (the employee's wife) claimed was caused by bullying behaviour at work. The Constitutional Court of the Czech Republic ruled that the employee's suicide did not meet the criteria of an accident at work because it was not caused by external, involuntary influences. The court stressed that the suicide was not committed in the course of or in direct connection with the performance of his work duties and that the suicide was therefore not directly linked to the alleged abusive behaviour of the plaintiff. The employee's psychiatric disorders, as established by expert evidence, were also taken into account. Without tying the employer's liability for the employee's suicide to the work-related injury, the absence of a provable causal link between the suicide and the work or working conditions is a bar to a successful employer liability claim.

¹⁰⁶ Labour Code, para. 220(1) and (2).

¹⁰⁷ As in para. 220(3) of the Labour Code in the context of an accident at work.

Summary

In Slovakia, the concept of hate speech has not been defined. The relevant literature is based on the case law of the ECtHR, which is based on the Recommendation of the Committee of Ministers of the Council of Europe. The recommendation defines hate speech as any form of expression that disseminates, promotes, justifies, or incites hatred based on racism, xenophobia, anti-Semitism, or other forms of intolerance. The Constitutional Court of the Slovak Republic has stated in a decision that it agrees with this definition and that the most common forms of hate speech in Slovakia are defamation and incitement to hatred.¹⁰⁸

The Constitution of the Slovak Republic declares that freedom of expression and the right to freedom of information is guaranteed to all. In addition, everyone has the right to express his or her opinion orally, in writing, in the press, in images, or in any other form, and the right to seek, receive and impart ideas and information freely, regardless of frontiers.¹⁰⁹ The Slovak Constitution, unlike the Hungarian Constitution, contains only enabling provisions on the exercise of freedom of expression, but no restrictive or prohibitive provisions.¹¹⁰ The Slovak Constitution also provides for an explicit prohibition of censorship and stipulates that freedom of expression and the right to seek and impart information may be restricted by law only if the measure is necessary in a democratic society to protect the rights and freedoms of others or if justified by the protection of national security, public order, public health or morals.¹¹¹

Although hate speech has not been defined, two forms of hate speech, defamation and incitement to hatred, are criminal offences. These are set out in paras. 423 and 424 of the Criminal Code, entitled “Defamation of nation, race and belief” and “Incitement to national, racial and moral hatred”. In Slovak legislation, there is no specific legal definition of cyberbullying, and the concept of cyberbullying is not defined, nor does the Criminal Code regulate or define the concept of cyberbullying.

The amendment of the Slovak Criminal Code, effective as of 1 July 2021, introduced a new offence of ‘dangerous electronic harassment’, which essentially covers the most serious cases of cyberbullying. Under the dangerous e-harassment definition, the most serious and dangerous cases of cyber-harassment are included, i.e., offences that aim to cause long-term, intentional damage

108 See the decision of the Constitutional Court No. PL ÚS 5/2017 of 9 January 2019.

109 Constitution of the Slovak Republic, Article 26(2).

110 Constitution of the Slovak Republic, Article 26(3).

111 Constitution of the Slovak Republic, Article 26(4).

to the victim's quality of life. Under the new provision, anyone who intentionally humiliates, abuses, unlawfully acts on behalf of another person or intentionally harasses another person in a persistent manner through an electronic communications service provider, computer network or system, is liable to imprisonment of up to three years. In addition, it is also a criminal offence to unlawfully publish or make available to another person a visual, audio or visual and audio recording of a personal speech obtained with the consent of the person concerned, provided that the recording is capable of endangering the dignity or otherwise seriously prejudicing the rights of the person concerned. In cases where the offender commits the offence with a specific motive (direct intent) or commits the offence against a protected person, the punishment is imprisonment from one to four years. If the offender causes substantial damage by committing the offence or commits the offence with the intention of obtaining a substantial benefit, or has been convicted of such an offence one or more times in the previous 24 months, he shall be punished with imprisonment for a term of between two and six years.¹¹²

In Slovakia, the following offences are also the most common in the context of cyberbullying: dangerous threats, dangerous persecution, production and distribution of child pornography, possession of pornographic recordings of children and participation in child pornography performances, endangering moral development, endangering the moral education of young people, extortion, coercion, sexual abuse, defamation.¹¹³

A study of the legislation in this area, as well as the laws, government decrees, and regulations issued by the various ministries, shows that they do not specifically address bullying in schools, but are merely internal, mainly informative, non-legislative materials. Among those already mentioned, Directive No. 36/2018 on the Prevention and Treatment of Bullying of Children and Pupils in Schools and Educational Institutions,¹¹⁴ which regulates the basic signs, forms, and manifestations of bullying of children and pupils, the possibilities of preventive measures and the methods of dealing with bullying of pupils, is not considered as legislation.

Neither international, nor EU, nor even national legislation defines the legal concepts of workplace bullying and cyberbullying. The research and the various sources are based on different definitions developed by other social sciences, such as bullying and other forms of bullying.

¹¹² Criminal Code, para. 360b.

¹¹³ See the relevant provisions of the Criminal Code, as described above.

¹¹⁴ *Smernica č. 36/2018 k prevencii a riešeniu šikanovania detí a žiakov v školách a školských zariadeniach.*

It should be noted, however, that in Slovakia there are a number of non-profit organisations dealing with the problem of cyberbullying, with websites where people can ask for help.

A major problem remains that Slovak legislation does not clearly define how crimes committed in the digital space are to be handled and prosecuted. In the context of cybercrime, the prosecution deals mainly with cases of child pornography, harassment, sexual abuse, and similar offences, as domestic legislation does not recognise other forms of online abuse and exploitation of children, such as sexting or hate speech. Legal regulation of internet broadcasters is much lighter than that of licensed traditional broadcasters. Act No. 308/2000 Coll. on Broadcasting and Retransmission, as amended, does not regulate all content on the internet, but only covers content broadcast over the internet and content that is part of on-demand audiovisual media services. Furthermore, the Slovak legal system does not specifically regulate social media platforms. The only legislation in force that has any direct relevance to the liability of social media is based on Act No. 22/2004 Coll. on Electronic Commerce, as amended, which was adopted to transpose the provisions of the e-commerce Directive into national law.

The Ministry of Education has an extensive network of counselling centres and the counselling services they provide; the child usually shows the first signs of problem behaviour long before he or she is referred to the social assistance services of the Department of Social Work; social and health service institutions are called upon when intervention is needed in the family and usually when comprehensive preventive activities initiated by the school need to be implemented; school and school facilities are often the only environment in which the positive influence of peers can be systematically corrected, especially in the case of disorganised individuals.

Traditional cases of cyberbullying show that if an employee suffers harm as a result of bullying behaviour at work, he or she can claim compensation through the institution of general employer's liability. According to the Labour Code, the employer is liable to the employee for damage caused to the employee by a breach of statutory obligations or intentional conduct contrary to good morals in the course of or directly connected with the performance of his/her duties. It is irrelevant in law whether the damage was caused by another employee, an employee acting on behalf of the employer or a third party.¹¹⁵

115 Labour Code, para. 192(1).

Bibliography

- Beznosková, P. (2020) 'Obťažovanie a šikana na pracovisku', *Práca, mzdy a odmeňovanie*, 2020/3-4.
- Bielik, P. (2022) 'Šikana v kybernetickom priestore a jej trestnoprávne dôsledky', *epravo.sk*, 2022 [Online]. Available online: <https://www.epravo.sk/top/clanky/sikana-v-kybernetickom-priestore-a-jej-trestnopravne-dsledky-5333.html>
- Boytha, Gy. (2008) 'A gyűlöletbeszéd polgári jogi szankcionálásának alapjogi keretei', *PJK*, 2008/1, pp. 10–20.
- Dolobáč, M. (2017) 'Technostres a ochrana duševného zdravia zamestnanca', *Pracovné právo v digitálnej dobe*, pp. 55–64.
- Erdősová, A. (2019) 'Nenávistný prejav a status obete z pohľadu rozhodovacej činnosti Európskeho súdu pre ľudské práva', *Správni právo*, pp. 448–460.
- Havrila, M. (2021) 'Šikana a kyberšikana v škole', *EPI odborné články*, 2021. [Online]. Available online: <https://www.epi.sk/odborny-clanok/sikana-a-kybersikana-v-skole.htm>
- Hulkó, G. (2021) 'Fake news és social media: szabályozás és közigazgatási intézkedések Szlovákiában', *In Medias Res*, 2021/2, pp. 297–311.
- Hulkó, G. (2021) 'The Impact of Digital Platforms and Social Media on Freedom of Expression and Pluralism in Slovakia', in Marcin Wielec (ed.): *The impact of digital platforms and social media on freedom of expression and pluralism*, Miskolc-Budapest: Central European Academy.
- Hollá, K. et al. (2017) *Prevenca kyberagresie a kyberšikanovania*. Nitra, Univerzita Konštantína Filozofa v Nitre.
- Hrašková, D. (2015) 'Šikana a kyberšikana v školstve', *EPI odborné články*, 2015. [Online]. Available online: <https://www.epi.sk/odborny-clanok/sikana-a-kybersikana-v-skolstve.htm>
- Izakovič, M. (2021) *Stalking – trestný čin nebezpečného prenasledovania*. Online elérhető: <http://www.pravnelisty.sk/clanky/a554-stalking-trestny-cin-nebezpecneho-prenasledovania>
- Kardos, T. (2007) 'Resiliencia u detí', in Zborník príspevkov z medzinárodnej vedeckej konferencie k 60. výročiu založenia Pedagogickej fakulty UK v Bratislave, Bratislava: Univerzita Komenského, Pedagogická fakulta, pp. 574–577.
- Kondorosi, F. (2015) 'A véleményszabadság nemzetközi jogi megítélésének paradigmaváltásai', *Acta Humana*, 2015/2, pp. 81–96.
- Kurucová, Z. (2018) 'Informačné a komunikačné technológie zneužíteľné na kyberšikanovanie (k pojmu a historickým súvislostiam)', *Magister Officiorum*, 2018/1, pp. 37–44.

- Lalík, T. (2016) 'Od strážnych psov k psom štváčom', *Justičná revue*, 2016/68, pp. 1054–1066.
- Minčíčová, M. (2021) Kyberšikana pri práci (nielen) v školskom prostredí, in Minčíčová, M., Dolobáč, M., Žulová, J. (eds.) *Zamestnanec v digitálnom prostredí*. Košice: Univerzita Pavla Jozefa Šafárika v Košiciach, Právnická fakulta.
- Parti, K. (2016) 'A megfélemlítés (bullying) szabályozása Magyarországon és külföldön', *In Medias Res*, 2016/1, pp. 114–146.
- Ružarovský, M. (2021) Trestný čin nebezpečného elektronického obťažovania. Available online: <https://www.ak-ruzarovsky.sk/index.php/2021/07/06/trestny-cin-nebezpecneho-elektronickeho-obtazovania/>
- Skácelová, L. (2003) 'Osobnost, dovednosti a techniky v primární prevenci' in Kalina, K. et al. (2003) *Drogy a drogové závislosti. 1. mezioborový přístup*. Praha: Úrad vlády České republiky.
- Šmigová, K. (2023) The Right to Privacy in the Digital Age from the Viewpoint of the Slovak Legal Order. in Marcin Wieleń (ed.) *The Right to Privacy in the Digital Age. Perspectives on Analysis of Certain Central European Countries' Legislation and Practice*. Miskolc–Budapest: Central European Academic Publishing, pp. 165–197.
- Švec, M. (2019) 'Šikanovanie na pracovisku', *Právo a manažment v zdravotníctve*, 1/2019, pp. 12–17.
- Vanc, M. (2021) Trestný čin nebezpečného elektronického obťažovania. Available online: <https://www.pravnenoviny.sk/trestny-cin-nebezpecneho-elektronickeho-obtazovania>
- Výborný, Š. (2013) *Nenávistný internet verzus právo*. Praha: Wolters Kluwer.
- Zgut, E., Denkova, A., Gabrizova, Z., Zbytniewska, K. (2021) Vajon készen áll a V4 egy kibertámadásra? Available online: https://www.politicalcapital.hu/konyvtar.php?article_read=1&article_id=2290
- Vágnerová, M. (1994) *Vývojová psychologie I: dětství a dospívání*. Praha: Karolinum.
- Valihorová, M., Surovcová, B. (2018) 'Kyberšikanovanie medzi žiakmi na primárnom stupni vzdelávania a ich sociálna osamelosť', *Školský psychológ/Školní psycholog*, 2018/19, pp. 42–51.

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

DE NEGRI LAURA

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

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

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

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

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

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

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

2. The regulation method of cyberbullying in Austria

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

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

2.1. *Hate speech in the offline space*

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

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

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

⁴ See Wickes et al., 2016.

⁵ See Perry, 2001.

⁶ Fuchs, 2021.

⁷ Fuchs, 2021, p. 12-13.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

15 Fuchs, 2021, p. 18-19.

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

17 Prohibition Act, Art. 3 d.

18 Prohibition Act, Art. 3 g.

19 Prohibition Act, Art. 3 h.

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

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

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

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

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

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

²¹ StGB Art. 283. (1).

²² StGB Art. 283. (2).

²³ StGB Art. 283. (3).

²⁴ StGB Art. 283. (4).

²⁵ Fuchs, 2021, p. 22.

²⁶ Fuchs, 2021, p. 28.

2.2. Hate speech in the online space

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

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

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

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

²⁷ Simsa, 2021, p. 18.

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

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

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

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

³² Austrian Civil Code (ABGB) Art. 20.

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

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

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

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

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

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

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

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

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

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

37 Communication Platforms Act.

38 Austrian Communications Authority.

39 Communication Platforms Act, Art. 1.

40 Communication Platforms Act, Art. 1.

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

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

2.3. *Hate speech in judicial practice*

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

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

⁴¹ Bodzási, 2021.

⁴² Bodzási, 2021.

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

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

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

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

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

3. Regulation of cyberbullying

3.1. Implementation of cyberbullying into the Austrian StGB

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

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

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

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

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

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

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

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

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

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

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

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

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

55 StGB Art. 115.

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

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

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

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

57 Reindl-Krauskopf, 2015, p. 19.

58 Reindl-Krauskopf, 2015, p. 19.

59 Tipold, 2017, p. 31.

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

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

62 Hatheuer (2021) p. 9.

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

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

3.2. Analysis of the facts

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

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

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

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

⁶⁵ StGB Art. 107c.

⁶⁶ StGB Art. 107c. (1)

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

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

3.3. Specific characteristics of the offence

3.3.1. Harassment by means of telecommunications or computer systems

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

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

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

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

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

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

70 StGB Art. 107 c.

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

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

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

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

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

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

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

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

⁷² Salimi, 2015, p. 191.

⁷³ Mitgutsch, 2020, p. 13.

⁷⁴ L. M. Hatheuer, 2021, p. 29.

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

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

3.3.4. *A qualified case of cyberbullying*

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

3.3.5. *Distinguishing cyberbullying from classic bullying*

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

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

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

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

⁷⁶ Salimi, 2015, p. 191.

⁷⁷ StGB Art. 107c. (2).

⁷⁸ Marzano, Lizut, 2019, p. 22.

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

3.3.6. *Further examples of cyberbullying*

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

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

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

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

⁷⁹ Katzer, 2014, p. 61.

⁸⁰ StGB Art. 105.

⁸¹ StGB Art. 111.

⁸² StGB Art. 115.

⁸³ StGB Art. 126 a.

⁸⁴ StGB Art. 152.

⁸⁵ StGB Art. 207a.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.1. The monitoring procedure

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

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

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

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

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

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

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

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

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

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

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

4.2. Cases of fines

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

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

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

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

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

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

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

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

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

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

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

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

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

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

4.3. Preventive legislation and practice

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

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

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

4.4. No hate speech movement

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

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

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

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

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

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

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

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

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

4.4.1. Saferinternet.at portal

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

4.4.2. Rat auf Draht¹¹⁰ or telephone advice

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

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

5. Responsibilities of service providers and institutions

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

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

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

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

111 Folk, 2021, p. 6.

112 Simsa, 2021, p. 19.

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

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

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

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

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

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

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

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

5.1. Reporting obligations for service providers

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

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

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

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

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

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

The report had to contain at least the following information:

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

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

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

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

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

5.2. Responsible agent and authorised agent for notification

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

This person:

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

5.3 Enforcement

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

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

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

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

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

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

Summary

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

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

¹²⁶ Janković, Stošić, 2022, p. 98.

¹²⁷ Gottschalk, 2022, p. 34.

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

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

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

Bibliography

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

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

XII. THE LEGAL APPROACH OF CYBERBULLYING IN GERMANY

NÓRA JAKAB

Introduction

The basis for regulating hate crime in Germany is EU Regulation 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the single market for digital services and amending Directive 2000/31/EC (Digital Services Act, DAS);¹ Grundgesetz für die Bundesrepublik Deutschland (GG)², Act on Improving Law Enforcement in Social Networks (NetzDG);³ Criminal Code (StGB);⁴ Code of Administrative Offences (OWiG);⁵ Code of Criminal Proce-

1 Official Journal of the European Union L 277/1, 27.10.2022. <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065>

2 Grundgesetz für die Bundesrepublik Deutschland in der im Bundesgesetzblatt Teil III, Gliederungsnummer 100- 1, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 1 des Gesetzes vom 20. Dezember 2024 (BGBl. 2024 I Nr. 439) geändert worden ist; <https://www.gesetze-im-internet.de/gg/GG.pdf>

3 Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG): Netzwerkdurchsetzungsgesetz vom 1. September 2017 (BGBl. I S. 3352), das zuletzt durch Artikel 29 des Gesetzes vom 6. Mai 2024 (BGBl. 2024 I Nr. 149) geändert worden ist; <https://www.gesetze-im-internet.de/netzdg/NetzDG.pdf>

4 Strafgesetzbuch (StGB): Strafgesetzbuch in der Fassung der Bekanntmachung vom 13. November 1998 (BGBl. I S. 3322), das zuletzt durch Artikel 2 Absatz 2 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist; <https://www.gesetze-im-internet.de/stgb/StGB.pdf>

5 Gesetz über Ordnungswidrigkeiten (OWiG): Gesetz über Ordnungswidrigkeiten in der Fassung der Bekanntmachung vom 19. Februar 1987 (BGBl. I S. 602), das zuletzt durch Artikel 10 des Gesetzes vom 12. Juli 2024 (BGBl. 2024 I Nr. 234) geändert worden ist; https://www.gesetze-im-internet.de/owig_1968/OWiG.pdf

dure (StPO);⁶ Guidelines on the imposition of fines by public authorities under the NetzDG.

‘Human dignity is inviolable. Its respect and protection are the duty of all public authorities.’ (Article 1(1) GG).⁷ It is indivisible and applies to all persons equally, regardless of their status. Since human dignity includes the requirement of equality of fundamental rights, racial discrimination or similar degradingly unequal treatment is a violation of Article 1(1) GG. In the case of prejudicial attacks against groups of people, each individual concerned is protected by Article 1(1) GG. However, the protection of dignity alone is too vague to provide a tangible constitutional framework for the prosecution of hate crimes. To make it concrete, account must be taken of the fundamental individual rights which all public authorities are obliged to respect (Article 1(3) GG).⁸ It follows from Article 1(1) GG that the principle of reasonable and proportionate punishment, measured by the principle of guilt, governs the field of public punishment. Discrimination based on religious or political views and other reprehensible aspects may violate Article 3(3), first sentence, GG, and therefore criminal offences cannot be based on these aspects.⁹ According to this provision, no one

6 Strafprozeßordnung (StPO): Strafprozeßordnung in der Fassung der Bekanntmachung vom 7. April 1987 (BGBl. I S. 1074, 1319), die zuletzt durch Artikel 2 Absatz 1 des Gesetzes vom 7. November 2024 (BGBl. 2024 I Nr. 351) geändert worden ist; <https://www.gesetze-im-internet.de/stpo/StPO.pdf>

7 Art 1 (1) Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt See also Zakariás, K. (2014). Human dignity does not only appear in the context of classical freedoms, but also in the context of the economic order or in other contexts. The constitutional recognition of human dignity in the Länder constitutions prior to the adoption of the Federal Constitution served as a building block for the human dignity article of the Grundgesetz. The early practice of the Bavarian Constitutional Court in relation to Article 100 of the Bavarian Constitution was particularly influential on the guarantee of human dignity in the Grundgesetz. The Bavarian Constitutional Court recognised that ‘[t]he human person is the bearer of the most precious spiritual and moral values and embodies a moral self-worth which cannot be lost and which is autonomous and untouchable against all political and legal interference by the state and society.’ The Parliamentary Council placed the requirement of respect for human dignity at the heart of the Grundgesetz ‘in order to express the spirit of the new state existence, in contrast to the state order that was destroyed in May 1945’. On this, see Zakariás, K. (2012).

8 Art 1 (3) Die nachfolgenden Grundrechte binden Gesetzgebung, vollziehende Gewalt und Rechtsprechung als unmittelbar geltendes Recht.

9 Art 3 (1) Alle Menschen sind vor dem Gesetz gleich. (2) Männer und Frauen sind gleichberechtigt. Der Staat fördert die tatsächliche Durchsetzung der Gleichberechtigung von Frauen und Männern und wirkt auf die Beseitigung bestehender Nachteile hin. (3) Niemand darf wegen seines Geschlechtes, seiner Abstammung, seiner Rasse, seiner Sprache, seiner Heimat und Herkunft, seines Glaubens, seiner religiösen oder politischen Anschauungen benachteiligt oder bevorzugt werden. Niemand darf wegen seiner Behinderung benachteiligt werden.

may be discriminated against or given preferential treatment on grounds of sex, gender, race, language, nationality and origin, religion or political opinions. No one shall be discriminated against on the grounds of disability.¹⁰

The general right of personality guarantees that everyone has the right to the free expression of his or her personality, provided that it does not infringe the rights of others and does not violate constitutional order or moral rules¹¹, which also takes the form of recognition of the dignity of the person and protection of personal honour (Article 2(1)(1) of GG). This, in connection with the offence of insult (§ 185 StGB)¹², may conflict with the freedom of expression enshrined in Article 5(1) of the GG¹³, when it comes to damaging the public image of the person concerned by making defamatory statements. The internet and social media have significantly expanded the forms in which hate crimes can be committed. The freedom of personal development guaranteed by Article 2(1) of the GG is infringed if the statements may damage the individual's reputation, weaken his or her social relations and thereby undermine his or her self-esteem. However, the freedom of expression under Article 5(1) of the GG also permits offensive statements in the public debate. In criminal law, this is expressed in the justification of insult offences based on safeguarding legitimate interests under § 193 StGB. In each individual case, the freedom of expression

¹⁰ Kugelmann, 2015, p. 14.

¹¹ Art 2 (1) Jeder hat das Recht auf die freie Entfaltung seiner Persönlichkeit, soweit er nicht die Rechte anderer erletzt und nicht gegen die verfassungsmäßige Ordnung oder das Sittengesetz verstößt.

¹² The right to the free development of the personality, guaranteed by Article 2(1) of the GG, occupies a special place among fundamental rights, in view of its close link with human dignity. The reason for this close link is that the essence of the human person is his dignity. 'It is because of his dignity that he [man] must be guaranteed the fullest possible development of his personality.' Although human dignity as a 'supreme constitutional principle' permeates Article 2(1) of the GG, as well as its other provisions, this does not mean that it does not have an independent content. Zakariás, 2014, p. 104.

¹³ Art 5 (1) Jeder hat das Recht, seine Meinung in Wort, Schrift und Bild frei zu äußern und zu verbreiten und sich aus allgemein zugänglichen Quellen ungehindert zu unterrichten. Die Pressefreiheit und die Freiheit der Berichterstattung durch Rundfunk und Film werden gewährleistet. Eine Zensur findet nicht statt. On the basis of the presentation of the normative content of human dignity and the general right of personality, we can conclude that individual honour – as a limitation of the freedom of opinion guaranteed by Article 5(1) of the GG, as referred to in Article 5(2) – may claim constitutional protection as a specific manifestation of the general right of personality, which is derived from the right to human dignity and the free development of personality. This is also supported by the literature. Accordingly, the right to individual honour – with the exception of the right to human dignity – may be restricted. Zakariás, 2014, p. 108.

of the person making the statement must be weighed against the person's claim to social esteem.¹⁴

In conclusion, the prosecution of hate crime is a matter of the state's duty to protect, rooted in fundamental rights. The focus is on the protection of human dignity¹⁵ (Article 1 GG) and the fight against discrimination (Article 3(3) GG). In view of the ultima ratio nature of state punishment, the need for a criminal law provision can only be confirmed in rare exceptional cases. The protection of bodily integrity or the right to social esteem, which is rooted in general rights of personality, is already adequately guaranteed by criminal law. Therefore, the legislator is under no constitutional obligation to extend protection against hate crime by law.¹⁶

1. Analysis of the Penal Code

A legal concept must be sufficiently defined. This applies even more so to criminal law, as every person must know whether a behaviour is punishable. According to Article 103(2) of the GG, a criminal offence is punishable only if criminal liability has been established by law before the offence was committed. The federal government's interpretation of the term is therefore based on this legislative understanding. It defines 'hate crimes' as crimes against a person because of 'political opinions, nationality, ethnicity, race, colour, religion, ideology, origin, sexual orientation, disability, physical appearance or social status'.¹⁷ Sec-

¹⁴ Kugelmann, 2015, p. 14.

¹⁵ Kinga Zakariás' position on the interpretation of Article 1 of the Grundgesetz is that the intention of the violator is irrelevant for the violation of human dignity, the conduct must be objectively capable of violating the human dignity of the individual. However, the link between the negative definition of human dignity (human beings must not be treated as objects) and the positive definition (human beings must be treated as subjects) is a way of clarifying the legal concept of dignity. The result of this link is that the violation of human dignity consists in calling into question the subject status of the human being and thereby reducing him or her to a mere object. Zakariás, 2014, p. 102.

¹⁶ Kugelmann, 2015, p. 14.

¹⁷ Kugelmann, 2015, p. 7. Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, (Gesetz über digitale Dienste, Digital Services Act, DAS); Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (NetzDG); Strafgesetzbuch (StGB); Ordnungswidrigkeitengesetz (OWiG); Strafprozessordnung (StPO); Leitlinien zur Festsetzung von Geldbußen im Bereich des Netzwerkdurchsetzungsgesetzes (NetzDG); Guidelines on setting regulatory fines within the scope of the Network Enforcement Act (Netzwerkdurchsetzungsgesetz – NetzDG)

tion 46 of the StGB regulates the principles of sentencing, according to which the court weighs the circumstances in favour of and against the offender when passing sentence. In particular, the following may be taken into account: the motives and aims of the offender, including in particular racist, xenophobic, anti-Semitic, gender-, sexual orientation- or other inhuman motives.¹⁸ The German government has highlighted the following criteria in the explanatory memorandum to the amendment of § 46 of the StGB: political opinion, nationality, ethnic origin, race, colour, religion, philosophical belief, origin, sexual orientation, disability, physical appearance or social status¹⁹. As the justification also guides the application of the law, the authorities and courts will use these criteria to interpret the criminalisation of racist, xenophobic or other inhuman motives and purposes.²⁰ An inhuman motive for a crime exists if the perpetrator has

18 StGB § 46 Grundsätze der Strafzumessung (2) Bei der Zumessung wägt das Gericht die Umstände, die für und gegen den Täter sprechen, gegeneinander ab. Dabei kommen namentlich in Betracht: die Beweggründe und die Ziele des Täters, besonders auch rassistische, fremdenfeindliche, antisemitische, geschlechtsspezifische, gegen die sexuelle Orientierung gerichtete oder sonstige menschenverachtende, ...

19 The final report of the German Bundestag's Committee of Inquiry into the NSU does not contain any specific recommendations for the judiciary to change substantive criminal law, but it does recommend that the police should thoroughly investigate any violent crime that may have a racial or other political motivation with regard to the victim's identity, and that this investigation should be documented in a clear and understandable way in the appropriate place. However, thorough examination and consideration of such motives should also be ensured in further proceedings, in particular in sentencing. In principle, the existing criminal law already meets this requirement, since § 46 of the German Criminal Code (StGB) requires the court to take into account not only the 'conduct resulting from the act' but also 'the motives and aims of the perpetrator' when sentencing, and it is generally recognised that this includes racist or xenophobic motives, but also other inhuman motives. However, the explicit inclusion of racist, xenophobic or other inhuman motives and aims in the catalogue of sentencing circumstances in § 46(2) sentence 2 of the StGB serves the purpose of emphasising the importance of these circumstances in sentencing. It is also intended to emphasise that the prosecution must also clarify and take account of these circumstances at an early stage of the investigation, since according to § 160(3) of the Code of Criminal Procedure (StPO) the prosecution's investigation must also cover circumstances relevant to the determination of the legal consequences of the offence. See on this: Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Umsetzung von Empfehlungen des NSU Untersuchungsausschusses des Deutschen Bundestage. RefE 2014-04-15 Umsetzung NSU-UA Empfehlungen (bundesgerichtshof.de) p. 6. 11-13.

20 Of course, the formulation as an illustrative list still allows the court to take into account motives and purposes other than those expressly mentioned when sentencing. Nor does it imply that racist, xenophobic or other inhuman motives and objectives are given one-sided weight in relation to the other punishment circumstances. It remains for the court to weigh the individual circumstances of punishment, if it is satisfied that they are relevant, in accordance with the recognised principles of sentencing, according to their importance and gravity in the particular individual case. The express mention of those

attacked the victim because of one of these criteria, a causal link must exist.²¹ In the context of § 46 of the StGB, a number of reprehensible characteristics can be included under the umbrella term of inhuman motive. The prohibition of discrimination in Article 3(3) of the GG may provide an approach to the definition of criminal offences.

As the term hate crime does not appear in the criminal law provisions, it should be understood as a generic term for certain manifestations of criminal offences. The fight against hate crime is part of the fight for human rights and fundamental freedoms²². In the Federal Republic of Germany, the concept of hate crime has the function of delimiting a type of crime which can be identified in criminal law and which, by its nature, requires special measures. This is due to the social relevance of hate crime, which is particularly harmful to peaceful coexistence and poses a specific criminal policy challenge. The measures concern prevention and repression. As regards criminal prosecution, a common understanding of the categorisation of hate crime by the police and the judiciary is needed to allow for a coherent assessment of offences, meaningful statistics and conclusive assessments.²³

In some cases, hate crime is understood to mean only violent crime. This may be related to the fact that statistical surveys or criminological studies often

motives in the second sentence of Paragraph 46(2) of the StGB does not therefore obscure the fact that the imposition of the sentence requires an overall view of the offence and the personality of the offender – as is not the case *de lege lata* with the mention of reparation and compensation for the victim – and does not diminish the importance of other sentencing circumstances, such as the culpable effects of the offence. The proposed addition also does not lead to an aggravating consideration of racist, xenophobic or other inhuman conduct as such. This would already contradict the clear wording of § 46 (2) sentence 2 of the StGB, which only allows for the consideration of attitudes expressed in the offence. Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Umsetzung von Empfehlungen des NSU Untersuchungsausschusses des Deutschen Bundestage. RefE 2014-04-15 Umsetzung NSU-UA Empfehlungen (bundesgerichtshof.de) p. 13.

21 See on this: Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Umsetzung von Empfehlungen des NSU Untersuchungsausschusses des Deutschen Bundestage. RefE 2014-04-15 Umsetzung NSU-UA Empfehlungen (bundesgerichtshof.de).

22 See about this: Hate crime | European Union Agency for Fundamental Rights (europa.eu) See also at international level the International Convention on the Elimination of All Forms of Racial Discrimination, adopted in New York on 21 December 1965, or the International Convention on the Prevention and Punishment of the Crime of Genocide, adopted on 9 December 1948.

23 Möglichkeiten effektiver Strafverfolgung bei Hasskriminalität Rechtsgutachten, p. 8. See also Glet, 2011.

focus on hate crimes motivated by right-wing extremism²⁴. However, the general social dimension of hate crime goes beyond violent acts based on right-wing extremist attitudes. Criminal law is essentially neutral and covers acts irrespective of the ideology of the perpetrator. The exception in § 130(4) StGB, which will be examined later, only reinforces this rule. Any motivation based on certain characteristics of the victim can lead to a classification as a hate crime. Not only persons holding extremist views can be considered as perpetrators, because such a narrow horizon may result in ‘ordinary’ manifestations of prejudice and attacks going unnoticed and therefore unaddressed. The perception of the victim is crucial in determining whether a crime is a hate crime.²⁵

§ 130 of the StGB deals with the offence of incitement of masses. According to (1), whoever, in a manner suited to causing a disturbance of the public peace, 1. incites hatred against a national, racial, religious group or a group defined by their ethnic origin, against sections of the population or individuals on account of their belonging to one of the aforementioned groups or sections of the population, or calls for violent or arbitrary measures against them or 2. violates human dignity of others by insulting, maliciously maligning or defaming one of the aforementioned groups, sections of the population or individuals on account of their belonging to one of the aforementioned groups or sections of the population incurs a penalty of imprisonment for a term of between three months and five years.

According to (2), whoever 1. disseminates content (section 11 (3)) or makes it available to the public, or offers, supplies or makes available to a person under 18 years of age content (section 11 (3)) which a) incites hatred against one of the

24 After the ‘National Socialist Underground Union’ (NSU) came to light in November 2011, it became clear that this right-wing terrorist group had managed to commit some of the most serious crimes for nearly fourteen years without detection by federal and state security authorities. An examination of the possible failings of the authorities responsible for constitutional protection, threat prevention and prosecution in the subsequent period in the area of criminal prosecution revealed the fact that investigations into crimes committed in several federal states were not carried out centrally by the police or the judiciary until the NSU came to light in November 2011. This may also have contributed to the fact that the links between the crimes and the links with far-right extremism and right-wing terrorism were only recognised after the NSU became known and the federal prosecutor general only took over the investigation afterwards. On this, see Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Umsetzung von Empfehlungen des NSU Untersuchungsausschusses des Deutschen Bundestages RefE 2014-04-15 Umsetzung NSU-UA Empfehlungen (bundesgerichtshof.de) p. 5–6.

25 Kugelmann, 2015, p. 11. See more: Bannenberg, B. Coester, M. and Marks, E. eds, 2005; Bannenberg, B. Coester, M. and Marks, E., 2004; Schneider, H. J., 2001; Schneider, H. J., 2003.

groups referred to in subsection (1) no. 1, sections of the population or individuals on account of their belonging to one of the groups referred to in subsection (1) no. 1, or sections of the population, b) calls for violent or arbitrary measures against one of the persons or bodies of persons referred to in letter (a) or c) attacks the human dignity of one of the persons or bodies of persons referred to in letter (a) by insulting, maliciously maligning or defaming them, or 2. produces, purchases, supplies, stocks, offers, advertises or undertakes to import or export content (section 11 (3)) as referred to in no. 1 (a) to (c) in order to use it within the meaning of no. 1 or to facilitate such use by another incurs a penalty of imprisonment for a term not exceeding three years or a fine.

According to (3) whoever publicly or in a meeting approves of, denies or downplays an act committed under the rule of National Socialism of the kind indicated in section 6 (1) of the Code of Crimes against International Law in a manner suited to causing a disturbance of the public peace incurs a penalty of imprisonment for a term not exceeding five years or a fine.

According to (4), Whoever publicly or in a meeting disturbs the public peace in a manner which violates the dignity of the victims by approving of, glorifying or justifying National Socialist tyranny and arbitrary rule incurs a penalty of imprisonment for a term not exceeding three years or a fine.

With regard to verbal hate crimes, insult offences under sections 185 et seq. of the StGB are considered to be criminal offences. A hate crime may be the subject of any offence under the Criminal Code if the offence is committed for a specific motive of the offender. With regard to offences that criminalise bias-based violence, in addition to classic violent crimes such as homicide, assault and sexual offences, any other offence that involves harming or threatening people, such as arson, coercion, robbery, extortion or hostage-taking, can also be considered.²⁶

2. Factual elements of certain hate crimes

The offences of insult are intended to protect personal honour and are governed in Germany by sections 185 et seq. of the StGB. The three basic offences are insult (StGB § 185), malicious gossip (StGB § 186, *üble Nachrede*) and defamation (StGB § 187).

²⁶ Kugelmann, 2015, p. 19.

According to § 185 of the StGB the penalty for insult is imprisonment for a term not exceeding one year or a fine and, if the insult is committed publicly, in a meeting, by disseminating content (section 11 (3)) or by means of an assault, imprisonment for a term not exceeding two years or a fine.²⁷

According to § 186 of the StGB, whoever asserts or disseminates a fact about another person which is suited to degrading that person or negatively affecting public opinion about that person, unless this fact can be proved to be true, incurs a penalty of imprisonment for a term not exceeding one year or a fine and, if the offence was committed publicly, in a meeting or by disseminating content (section 11 (3)), a penalty of imprisonment for a term not exceeding two years or a fine. Under § 187 StGB, whoever, despite knowing better, asserts or disseminates an untrue fact about another person which is suited to degrading that person or negatively affecting public opinion about that person or endangering said person's creditworthiness incurs a penalty of imprisonment for a term not exceeding two years or a fine, and, if the act was committed publicly, in a meeting or by disseminating content (section 11 (3)), a penalty of imprisonment for a term not exceeding five years or a fine.²⁸

According to § 188 if an offence of insult (section 185) is committed publicly, in a meeting or by disseminating content (section 11 (3)) against a person involved in the political life of the nation on account of the position that person holds in public life and if the offence is suited to making that person's public activities substantially more difficult, the penalty is imprisonment for a term

27 Insult is usually understood as an attack on another person's honour through a display of contempt or disrespect for the other person. Insult is generally characterised by the expression of a value judgment (i.e. opinion) against the person concerned or a third party which cannot be proven. This distinguishes it from the offences of malicious gossip (StGB § 186) and defamation (StGB § 187), which relate to statements of fact. The prevailing view, however, is that the statement of fact can be punished as an insult under Section 185 StGB, even if it is addressed to the victim himself ('you stole my watch!'). However, it must then be proved that the statement is untrue. A true statement of fact can only be punishable under § 192 StGB in exceptional cases if it is a so-called 'formal offence', i.e. if the alleged fact is true but the offensive character is due to the form of the statement. The insult must not have any negative consequences for the person concerned beyond defamation. See on this: Grundzüge der Beleidigungsdelikte (§§ 185 ff. StGB) aus straf- und zivilrechtlicher Sicht. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 052/22, p. 4.

28 A common feature of both offences is that criminal liability can be excluded if the alleged fact is proven (cf. StGB § 190). The person concerned must generally tolerate confrontation with the actual fact, unless it constitutes an official insult within the meaning of StGB § 192. Moreover, the defamatory fact must be capable of 'disparaging or degrading the person concerned in the eyes of the public' or, in the case of defamation, of endangering his or her credibility. Grundzüge der Beleidigungsdelikte (§§ 185 ff. StGB) aus straf- und zivilrechtlicher Sicht. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 052/22, p. 5.

not exceeding three years or a fine. The political life of the nation reaches down to the local level. According to (2) malicious gossip (section 186) under the same conditions incurs a penalty of imprisonment for a term of between three months and five years and defamation (section 187) under the same conditions incurs a penalty of imprisonment for a term of between six months and five years.

It is emphasised that according to § 11 (3) StGB for the purposes of those provisions which refer to this subsection, ‘content’ means that which is contained in writings, on audio or visual media, on data carriers, in images or other materialised content or which is also transmitted independently of any storage using information or communication technologies.

In the case of offences of insult, malicious gossip and defamation, the offence is qualified if it is committed in public, at a meeting or by disseminating content (Article 11(3)). The content may be transmitted by means of information or communication technology. The offences do not explicitly mention an infocommunication technology as a means of commission, there is no reference to online space as a place of commission, and the legislator has avoided formulating the result.

According to § 201 of the StGB, in the case of a violation of privacy of spoken word whoever, without being authorised to do so, 1. makes an audio recording of the privately spoken words of another or 2. uses or makes a recording thus produced available to a third party incurs a penalty of imprisonment for a term not exceeding three years or a fine.

According to § 201a of the StGB, in the case of violation of intimate privacy and of rights of personality by taking photographs or other images whoever

1. without being authorised to do so creates or transmits photographs or other images of another person in private premises or in a room which is specially protected from view, and thereby violates the intimate privacy of the person depicted;
2. without being authorised to do so produces a photograph or other image exhibiting the helplessness of another person or transmits such image, and thereby violates the intimate privacy of the person depicted;
3. without being authorised to do so creates or transmits a photograph or other image which in a grossly offensive manner exhibits a deceased person;
4. uses a photograph or other image produced by an offence under no. 1 to no. 3 or makes it available to a third party or
5. makes available to a third party, in the awareness of lacking authorisation to do so, a photograph or other image of the type set out in no. 1 to no. 3 which was produced with authorisation, and, in the cases under no. 1 and no. 2, thereby violates the intimate privacy of the person depicted,

incurs a penalty of imprisonment for a term not exceeding two years or a fine.

According to § 240 of the StGB, in the case of coercion (Nötigung) whoever unlawfully, by force or threat of serious harm, compels a person to do, acquiesce to or refrain from an act incurs a penalty of imprisonment for a term not exceeding three years or a fine.

According to § 241 of the StGB, in the case of threatening commission of serious criminal offence whoever threatens a person with the commission of an unlawful act against sexual self-determination, physical integrity, personal liberty against that person or a person close to him or her or against an object of significant value incurs a penalty of a term of imprisonment not exceeding one year or a fine. If the act is committed publicly, in a meeting or by disseminating content (section 11 (3)), the penalty in the cases under subsection (1) is a term of imprisonment not exceeding two years or a fine and in the cases under subsections (2) and (3) a term of imprisonment not exceeding three years or a fine.

The offences do not explicitly mention any infocommunication technology as a means of commission, there is no reference to the online space as a place of commission, and the legislator avoided formulating the result. However, these offences can also be committed in the online space.

2.1. Hate-mongering insult

Section 192a of StGB deals with hate-mongering insult, which was newly introduced into the German Criminal Code in September 2021. Its purpose is to close the gap that previously existed in criminal liability for sending hateful content to the persons concerned.

According to the statement of facts, whoever allows content (section 11 (3)) suited to violating the human dignity of others by insulting, maliciously maligning or defaming a group defined by its national, racial, religious or ethnic origin, ideology, disability or sexual orientation or individuals on account of their belonging to one of these groups to come to the attention of another person who belongs to one of the aforementioned groups without having been requested to do so by that person incurs a penalty of a term of imprisonment not exceeding two years or a fine.

The act must be capable of offending the human dignity of others. The fact that one of the groups protected by § 192a of StGB or a person must be insulted,

maliciously gossiped or defamed because of his/her membership of one of these groups is in accordance with § 130(1) StGB.²⁹

While the requirement of offence against human dignity in the context of hate speech is only intended to exclude simple defamation offences, § 192a StGB has an additional function. The legislator rightly assumes that an offence against human dignity can be committed by confronting a group with serious, non- or insufficiently individualised statements if the addressee is linked to the group by some identity-forming characteristic. The suitability clause is also aimed at this link and thus has a ‘double filtering function’ in terms of content. With regard to the element of association with a group, it may exceptionally exclude from the scope of the offence content which incites with sufficient intensity against one of the listed groups, but which is not capable of violating individual human dignity.³⁰

With regard to § 130 Section (1) no 2 of the StGB, Hörnle explains the choice of the term ‘insult’ by the additional limitation that ‘the insult must relate expressly and primarily to defamation.’ However, since the term ‘insult’ in § 192a StGB refers to the content and not to the person making the statement, there can be no limiting effect here anyway. According to Streng’s interpretation, § 130 Section (1) no. 2 of the StGB does not speak of an insult to human dignity because it is often only through the conduct of inciting third parties and not through the statement itself, but in the case of § 192a of StGB the insult is directly caused by confrontation with the content, there is no need for mediation through the violent acts of third parties.³¹

According to the reasoning, the quality of the punishable content is determined on the basis of § 130 Section (2) no. 1 (c) of the StGB, which implicitly refers to the group characteristics in § 130 Section (1) no. 1 of the StGB. It is striking that the offence of incitement to hatred also refers to national, racial, religious and ethnic group characteristics, but not to ideology, disability or sexual orientation. However, these groups can be included in the protected circle of § 130 Section (1) no. of the StGB, provided that the groups are sufficiently distinct and are quantitatively decisive. Incitement to hatred does not have this openness; the list of group characteristics is exhaustive and constitutive of criminal relevance. This difference can be explained by the different protection objectives of the offences: the prevailing view is that the offence of incitement to hatred is intended to protect public peace and human dignity in the abstract – both of which can in principle be threatened by incitement of masses of any group of the

²⁹ Nussbaum, 2021, p. 335.

³⁰ Nussbaum, 2021, p. 338.

³¹ Nussbaum, 2021, pp. 338–339.

population – whereas § 192a of the StGB focuses on the protection of individual human dignity. Although an offence against individual dignity can of course occur without reference to any of the characteristics listed in § 192a of the StGB, the basic idea behind the new criminal law provision is that an offence against the individual dignity of the recipient of the content is only possible if he or she is linked to the group by an identity-forming characteristic.³²

In the case of this offence, the offence does not explicitly include any information technology as a means of commission, there is no reference to online space as a place of commission, the legislator avoided formulating the result, while at the same time making available as a conduct may include content that is capable of violating human dignity, which is transmitted by means of information and communication technology. The offence of incitement of masses is the unsolicited making available, which is defined in the Explanatory Memorandum by the terms sending, offering and making available. In contrast to Section 185 of the German Criminal Code, the offence does not require the actual knowledge of the addressee, but the mere possibility is sufficient. It is clear from the legislative material that the offence also includes the act of ‘remotely communicating’. This wording raises questions, given that the act of ‘remotely verbal’ refers to content within the meaning of § 11(3) StGB. It is true that the concept of content, which has replaced the concept of writing, no longer necessarily requires content to be embodied, but also includes content that is transmitted independently of storage by means of information and communication technology, including words transmitted by telephone. It does not, however, include verbal expressions that do not require technical transmission, even if the human dignity of the members of the group present may be equally violated. The notion of ‘making available’ must be interpreted accordingly and is not limited to the transfer of the right to dispose of embodied content.³³

2.2. Stalking

Section 238 of the StGB regulates the offence of stalking. According to (1), whoever, without being authorised to do so, stalks another person in a manner suited to not insignificantly restricting that person’s lifestyle by repeatedly

1. seeking the other person’s physical proximity,
2. trying to establish contact with the other person by means of telecommunications or other means of communication or through third parties,

³² Nussbaum, 2021, p. 339.

³³ Nussbaum, 2021, p. 340.

3. improperly using the other person's personal data for the purpose of
 - a) ordering goods or services for that person or
 - b) inducing third parties to make contact with that person,
4. threatening the other person, one of his or her relatives, or someone close to him or her with causing injury to life or physical integrity, health or liberty,
5. committing an unauthorised access or preparation of an unauthorised access to data pursuant to § 202a, § 202b or § 202c to the detriment of that person, a relative or another person close to that person,
6. disseminating or making available to the public a depiction of that person, one of his or her relatives or another person close to him or her,
7. disseminating or making available to the public content (section 11 (3)) suited to disparaging or negatively affecting public opinion about that person by feigning that person's authorship or
8. committing an act comparable with nos. 1 to 7.

According to (2), in particularly serious cases under subsection (1) nos. 1 to 7, stalking incurs a penalty of imprisonment for a term of between three months and five years. An especially serious case typically occurs where the offender

1. by committing the offence causes damage to the health of the victim, a relative of or another person close to the victim,
2. places the victim, a relative of or another person close to the victim in danger of death or at risk of serious damage to health on account of the act,
3. stalks the victim by committing a large number of acts constituting an offence over a period of at least six months,
4. uses a computer program in the commission of an act constituting an offence under subsection (1) no. 5 whose purpose is to digitally spy on other persons,
5. uses a depiction obtained through one of the acts constituting an offence under subsection (1) no. 5 in the commission of an act constituting an offence under subsection (1) no. 6,
6. uses content (section 11 (3)) obtained through one of the acts constituting an offence under subsection (1) no. 5 in the commission of an act constituting an offence under subsection (1) no. 7 or
7. is over 21 years of age and the victim is under 16 years of age.

It can therefore be seen that so far only the offence of stalking (StGB § 238) explicitly mentions telecommunication – which includes digital forms of communication – as a possible means of committing the offence (StGB § 238 Section (1) no. 2).

In this way, there is an implicit reference to online space as a ‘place of offence’, but the wording of the offence does not imply that it is exclusively online, only that stalking can be committed online.

Stalking may also be committed by disseminating or making available to the public content (Section 11(3)) that is likely to defame or degrade the person in the eyes of the public. This does not explicitly include any infocommunication technology as a means of offence, there is no reference to online space as a place of offence, the legislator has avoided formulating the result, but making available as an offence may include content that is capable of offending human dignity and is transmitted by means of information and communication technology. In this respect, the offence of committing an offence in the online space may also be a qualified case.

2.3. *Cybercrime*

Germany was one of the first countries in the world to introduce criminal measures against cybercrime. This mainly concerns the crimes of data modification (StGB § 303a), computer sabotage (StGB § 303b) and data espionage (StGB § 202a). In addition, there is computer forgery (§§ 269, 270 StGB) and computer fraud (§ 263a StGB). Data security protection rules also exist in data protection law.³⁴

Certain crimes are increasingly committed using the internet and electronic forms of communication. In recent years, therefore, ‘cybercrime’ has increasingly become a focus of attention for security authorities and politicians. However, the focus should be on certain types of crime which experience has shown to be particularly affecting the human dignity of the victims of crime: insults, harassment, coercion, threats and extortion. However, these crimes do not specifically mention digital forms of crime.

Cybercrime can include the following criminal offences:

- StGB § 174-184 Criminal law offences relating to the protection of sexual autonomy
- StGB § 185 insult (§ 185)
- StGB § 186 malicious gossip
- StGB § 187 defamation
- StGB § 192a hate-mongering insult,

³⁴ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017 (BGBl. I S. 3352) <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html> 1. § (3). [https://www.bidt.digital/glossar/cyberkriminalitaet/#::~:~:text=Deutschland%20hat%20als%20eines%20der,Daten%20\(%C2%A7%20202a%20StGB\).](https://www.bidt.digital/glossar/cyberkriminalitaet/#::~:~:text=Deutschland%20hat%20als%20eines%20der,Daten%20(%C2%A7%20202a%20StGB).)

- StGB § 201 violation of privacy of spoken word
- StGB § 201a violation of intimate privacy and of rights of personality by taking photographs or other images StGB § 238 stalking
- StGB § 240 coercion
- StGB § 241 threatening commission of serious criminal offence
- Art Copyright Act (Kunsturheberrechtsgesetz) § 33 Criminal offences against the copyright in works of art and photography³⁵

Thus, only the offence of stalking (StGB § 238) explicitly mentions telecommunication – which includes digital forms of communication – as a possible means of committing the offence (StGB § 238 Section (1) no. 2.). A person who, without authorisation, stalks another person in a manner likely to seriously disrupt the life of that person by persistently using a means of telecommunication or other means of communication or by attempting to contact that person through a third party is punishable by a term of imprisonment not exceeding three years or a fine (...) Digital content that constitutes an offence of insult (StGB § 185) or threat (StGB § 241) is subject to the Act on the Improvement of Law Enforcement in Social Networks (NetzDG).³⁶ It is aimed at telemedia service providers and imposes reporting and monitoring obligations with fines for relevant offences.

2.4. Action against online hate crime, service provider responsibility

The online debate culture is often aggressive, abusive and hateful. Hate crimes can affect anyone based on their opinion, colour, origin, religion, gender or sexual orientation. The fight against punishable hate speech on social networks has also become a high priority in Germany. Law enforcement on social networks must therefore be improved to ensure that objectively punishable content such as hate speech, insults and defamation is removed immediately. The growing incidence of hate crime, particularly on social networks such as Facebook, YouTube and Twitter, prompted the Federal Ministry of Justice and Consumer Protection to set up a working group of network operators and civil society representatives back in 2015. The companies represented in the task force committed to improve

35 Handlungsansatz zur Prävention und Intervention von Cybermobbing. Vom Mobbing zum Cybermobbing. <https://www.klicksafe.de/cybermobbing/handlungsansatz-zur-praevention-und-intervention-von-cybermobbing>; p. 45. 46. https://www.klicksafe.de/fileadmin/cms/download/Sonstiges/Themen/Cybermobbing/Kapitel2_Vom_Mobbing_zum_CyberMobbing.pdf

36 ‘Cyberkriminalität’ Strafrechtliche Regelungen in Deutschland und ausgewählten EU-Mitgliedstaaten, Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 039/19, p. 4-5.

the handling of hate crime reports on their sites, to establish user-friendly mechanisms for reporting critical posts, and to review the majority of reported posts within 24 hours by linguistically and legally trained teams and delete them if they are illegal. An audit of social network deletion practices carried out by jugendschutz.net in January/February 2017 showed that user complaints about hate crime are still not being processed promptly and adequately. YouTube now deletes criminal content 90% of the time. In contrast, Facebook deletes content only 39% of the time and Twitter only 1% of the time. Social network providers have a responsibility to fulfil. Given that existing tools and voluntary commitments promised by social networks are not effective enough and that there are significant problems with the enforcement of applicable law, compliance rules for social networks are needed to ensure that they can effectively and promptly tackle online hate crime.³⁷

On 1 September 2017, the law on improving law enforcement in social networks (Netzwerkdurchsetzungsgesetz, NetzDG) entered into force.³⁸ According to (1), the Act applies to telemedia service providers that operate for profit platforms on the Internet that are designed to allow users to share any content with other users or to make it available to the public (social networks). Platforms with journalistic/editorial content for which the service provider itself is responsible are not considered social networks. The same applies to platforms for individual communication or for the distribution of specific content. According to (3), unlawful content is content that is in breach of § 86 (dissemination of propaganda material of unconstitutional and terrorist organisations), § 86a (use of symbols of unconstitutional and terrorist organisations), § 89a (preparation of serious violent offence endangering the state), § 91 (instructions for committing serious violent offence endangering state), § 100a (treasonous forgery), § 111 (Public incitement to commit offences), § 126 (Disturbing public peace by threatening to commit offences), § 129-129b (Forming criminal or terrorist organisations), § 130 (incitement of masses), § 131 (depictions of violence), § 140 (rewarding and approval of offences), § 166 (Revilement of religious faiths and religious and ideological communities), § 184b (Dissemination, procurement and possession of child pornographic content), § 185-187. (insult, malicious gossip, defamation), § 189 (defiling memory of dead), § 201a (violation of intimate privacy and of rights

³⁷ Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, https://netzpolitik.org/wp-upload/2017/03/1703014_NetzwerkDurchsetzungsG.pdf

³⁸ Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017 (BGBl. I S. 3352) <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>

of personality by taking photographs or other images), § 241 (coercion) or § 269 (forgery of data of probative value) and cannot be justified.

A complaint about unlawful content under subsection (4) is any objection to content that requests the removal of the content or the blocking of access to the content, unless the complaint does not clearly allege that the content is unlawful.

According to § 1 (2), the provider of a community network is exempted from the obligations laid down in the Act if the community network has fewer than two million registered users in Germany.

According to § 2 (1), social network service providers that receive more than 100 complaints about illegal content in a calendar year are obliged to produce a report in German³⁹ every six months on the handling of complaints about illegal content and to publish it in the Federal Gazette and on their website no later than one month after the end of the six-month period. The report published on their website must be easily recognisable, directly accessible and permanently available. The report shall include, inter alia, information on whether and to what extent academics and researchers have been given access to the provider's data during the reporting period in order to carry out an anonymised assessment, the nature, main features and scope of the procedures used to automatically detect content to be removed or blocked. These are the procedures for the control of content.

According to § 3, the social network service provider must provide an effective and transparent, easily identifiable, directly accessible, easy to use and

39 Paragraph (2) summarises in 17 points what aspects, at least, the report must cover. For example:

1. General information on the efforts made by the social network provider to prevent crime on the platforms.
2. The nature, main features and scope of the procedures used to automatically detect content to be removed or blocked.
3. A description of the mechanisms for submitting complaints about illegal content, the criteria for deciding whether to remove or block illegal content, and the review procedure, including the order of review in which the review will be conducted in relation to the existence of illegal content or a breach of the contractual provisions between the provider and the user.
4. The number of complaints received during the reporting period about illegal content, broken down by complaints bodies and users, and the reason for the complaint.
5. The organisation, staffing, technical and linguistic competence of the complaints handling units, and the training and support of the persons responsible for complaints handling.
6. Membership in industry associations, indicating whether there is a complaints office in these industry associations.
7. Number of complaints for which an external body was consulted to prepare the decision.

permanently available procedure for the submission of complaints about illegal content. According to Article 3b, the social network service provider must provide an effective and transparent procedure for both the complainant and the user on whose computer the illegal content has been stored to initiate a review of the decision to remove or block access to the content (the original decision) taken in response to a complaint about illegal content. The procedure ensures that the social network provider

1. immediately takes note of the complaint and checks whether the content reported in the complaint is illegal and whether it should be removed or access to it should be denied;
2. removes or blocks access to the manifestly illegal content within 24 hours of receiving the complaint; this does not apply if the social network has agreed with the competent law enforcement authority to remove or block the manifestly illegal content for a longer period;
3. removes or disables access to the illegal content without undue delay, normally within seven days of receipt of the complaint; the seven-day time limit may be exceeded if
 - (a) the decision on the illegality of the content depends on the falsity of a factual statement or on other cognizable factual circumstances; in such cases, the social network may give the user the opportunity to comment on the complaint before taking a decision;
 - (b) within seven days of receipt of the complaint, the community network provider shall refer the decision of illegality to a self-regulatory body and submit to its decision.

According to § 3a, the provider of the social network is obliged to forward such content to the Federal Office of Criminal Investigation as the central office for the purpose of enabling the prosecution of criminal offences,

1. which has been reported to the service provider as illegal content;
2. which has been removed or access to which has been blocked by the service provider, and
3. for which there are concrete indications that at least one of the offences is being committed
 - a) offences as defined in §§ 86, 86a, 89a, 91, 126, 129-129b, 130, 131 or 140 of the StGB;
 - b) § 184b of the StGB, or
 - c) violation of § 241 of the StGB in the form of a threat to commit a crime against life, sexual self-determination, bodily integrity or personal liberty, and cannot be justified.

According to § 3c, the supervisory body may recognise private law bodies as conciliation bodies for the out-of-court settlement of disputes between complainants or users who store infringing content and social network service providers.

According to § 4, a deliberate or negligent breach of the obligations laid down in the Act is punishable by administrative penalties and fines of up to EUR 500 000 or EUR 5 000 000 million. According to § 4, the administrative authority within the meaning of § 36 Section (1) no. 1. of the Administrative Offences Act is the Federal Office of Justice. The Federal Ministry of Justice and Consumer Protection shall, in agreement with the Federal Ministry of the Interior, Building and Community Affairs, the Federal Ministry of Economic Affairs and Energy and the Federal Ministry of Transport and Digital Infrastructure, issue general administrative principles on the exercise of discretion by the administrative authority when initiating the fine proceedings and when imposing the fine.⁴⁰

§ 4a provides for the supervisory body. The Federal Office of Justice is the administrative authority responsible for monitoring compliance with the provisions of the Act. If it finds that a provider of a social network has violated or is violating the provisions of the Act, it shall take the necessary measures against the provider. In particular, it may order the provider to cease the infringement.

According to § 5, social network providers are obliged to designate a domestic delivery agent and to draw attention to it on their platform in an easily recognisable and directly accessible way. Service of process is important in fines and surveillance proceedings and in court proceedings before German courts for dissemination of illegal content or for unfounded allegations of such dissemination, in particular in cases where the restoration of removed or blocked content is requested, service may be made on him or her. This also applies to service of documents instituting such proceedings, service of final judicial decisions and service in enforcement or execution proceedings.

The law was amended on 3 April 2021 for reporting obligations and on 28 June 2021 for video-sharing platforms.

⁴⁰ For more on platform responsibility, see also: <https://www.eff.org/de/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments>

3. Protection of minors

The criminal protection of minors against sexual violence on the internet is based on the criminal law provisions on the protection of sexual self-determination (StGB §§ 174-184), while cyberbullying, as mentioned, can be based on several criminal law provisions, such as insult (StGB § 185) or criminal infringement of the rights to effigy (§ 33 of the Copyright Act on Visual Art and Photographic Works).⁴¹

Sexual violence against minors on the internet is punishable, in particular the offering of children for sexual abuse, sexual abuse of children without physical contact and the preparation of sexual abuse of children. Any person under the age of fourteen is considered a child (StGB § 176 Section (1) no. 1).⁴²

According to § 176 (1) whoever 1. performs sexual acts on a person under 14 years of age (child) or has the child perform sexual acts on them, 2. causes a child to perform sexual acts on a third person or to have a third person perform sexual acts on them, 3. offers or promises to supply a child for an offence under no. 1 or no. 2 incurs a penalty of imprisonment for a term of at least one year.

According to Section (2) in the cases under subsection (1) no. 1, the court may dispense with imposing a penalty in accordance with this provision if the sexual act between the offender and the child was consensual and the difference both in age and level of development and maturity is small, unless the offender is exploiting the child's lack of capacity for sexual self-determination.

§ 176a StGB criminalises sexual abuse of children without physical contact. Accordingly, whoever performs a sexual act in front of a child or causes a third person to perform a sexual act in front of a child is punishable by imprisonment for a term of between six months and ten years (StGB § 176 (1) no. 1., point 1.). StGB § 184h stipulates that sexual acts require a significant violation of a protected legal interest (StGB § 184h. § no. 1. point 1.) and that the sexual acts performed in front of a person must be actually perceived by another person (StGB § 184h no. 2 point 2). It is sufficient if the sexual acts are transmitted to the

41 Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III, Gliederungsnummer 440-3, veröffentlichten bereinigten Fassung, das zuletzt durch Artikel 3 § 31 des Gesetzes vom 16. Februar 2001 (BGBl. I S. 266) geändert worden ist. Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 4.

42 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 4.

victims via the Internet and it is possible to follow the acts on a screen. However, it is necessary that the perpetrator has an explicit interest in the victim's perception.⁴³

In addition, § 176a (1) no. 3 point 3 of StGB punishes anyone who influences a child with pornographic content or inappropriate speech. Content is pornographic if it depicts sexual events in a crude form and without any connection to other manifestations of life. The offence of influence requires a deeper psychological influence on the victim, for example by arousing age-inappropriate sexual interest. Nor is physical proximity between the offender and the victim necessary in this respect.⁴⁴

According to § 176b Section 1 no. 1 of the StGB, a person who influences a child with the content of § 11(3) StGB in order to induce the child to perform a sexual act with or in front of the perpetrator or a third person is punishable by imprisonment of between three months and five years. The offence is intended to criminalise the initiation of sexual acts and includes, for example, influencing children in internet chat rooms with the intention of future sexual acts. Targeting minors in this way to initiate sexual contact on the internet is known as 'cybergrooming'. Similarly, influencing a child with content in order to produce or obtain child pornography content or to obtain possession of such content is punishable (StGB § 176b Section 1 no. 2).⁴⁵

According to § 176e (1) of the StGB, anyone who distributes or makes available to the public content which is capable of serving as an instruction to commit an unlawful act as defined in §§ 176-176d StGB and which is intended to incite others to commit such an act or to create a disposition to commit such an act is also punishable by imprisonment of up to three years or a fine. The offence is therefore the dissemination and making available to the public of content which is capable of serving as an incitement to commit the offences of abuse referred to in § 176 to 176d of the StGB. Finally, under § 176e Section 3 of the StGB, a person who obtains, possesses, makes available to another person or obtains for another person such instructions is punishable by imprisonment for up to two years or a fine. In addition, § 184b Section 1 sentence 1, no.s 1 to 4 of the StGB

43 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 5.

44 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 5.

45 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 6.

punishes the distribution, making available, inducing to possess, producing, possessing, obtaining and supplying child pornography content with a prison sentence of up to one to ten years⁴⁶.

If a person's effigy is published or displayed without consent (§ 22 of the Copyright of Works of Art and Photographic Works Act, KUG) or other justification (§ 23 of the Copyright Act, KUG) as a result of cyberbullying, *criminal liability* may be incurred under § 33 Section 1 of the Copyright Act, which provides for imprisonment for up to one year or a fine. A portrait of a person is a portrait if the appearance of a person is reproduced in such a way that the person has reasonable grounds to believe that he or she is recognised in the circle of acquaintances. If, unlike cyberbullying, the perpetrator seeks to contact the person concerned by stalking the victim without permission and on a sustained basis by means of communication ('cyberstalking'), this may ultimately be punishable under § 238 Section 1 no. 2 of StGB.⁴⁷

The offences do not explicitly mention any infocommunication technology as a means of commission, there is no reference to the online space as a place of commission, and the legislator avoided formulating the result. However, these offences can also be committed in the online space.

In addition to the criminal law provisions, the German Youth Protection Act (JuSchG)⁴⁸, the Interstate Treaty on the Protection of Minors in the Media (JMStV)⁴⁹ and the Act on Improving Law Enforcement in Social Networks (NetzDG) contain provisions on the protection of minors on the internet.

According to § 1 of the Interstate Treaty on the Protection of Human Dignity and the Protection of Minors in Broadcasting and Telemedia (JMStV)⁵⁰, the purpose of the interstate treaty is to provide uniform protection for children and young people against content in electronic information and communication media that is harmful to their development or education, and against content

46 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 7.

47 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 8–9.

48 Jugendschutzgesetz vom 23.07.2002 (BGBl. I S. 2730), das zuletzt durch Artikel 1 des Gesetzes vom 09.04.2021 (BGBl. I S. 742) geändert worden ist.

49 Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) vom 13.09.2002, zuletzt geändert durch Artikel 2 des Zweiten Medienänderungsstaatsvertrages vom 14./27.12.2021 als Anlage des Gesetzes vom 31.03.2022).

50 <https://www.gesetze-bayern.de/Content/Document/JMStV>

in electronic information and communication media that is harmful to human dignity or other legal interests protected by the Criminal Code.

According to § 24a of the JuSchG, service providers who store or provide third-party information for profit must take precautionary measures to ensure that the media protection objectives for children and young people (JuSchG § 10a) are met. Precautionary measures include the provision of reporting and redress procedures (JuSchG § 24a (2) no.s 1, 2), easy-to-find links to independent advice, assistance and reporting facilities (JuSchG § 24a (2) no. 5.) and to establish basic settings limiting the risks of use for children and young people (JuSchG § 24a (2) no. 7). These requirements also apply to providers of social networking and messaging services, whether or not they are established in Germany (JuSchG § 24a (4), 1st sentence). However, service providers whose services can be shown to be used by fewer than one million users in Germany are exempted from the obligations (JuSchG § 24a (3)). JuSchG § 16 sentence 2 further provides that the specific requirements on telemedia content are to be taken over from the JMStV. The term telemedia generally refers to all information and communication services, unless they are subject to specific requirements as telecommunications services, telecommunications protected services or broadcasting services (Telemedia Act⁵¹). The JMStV defines, for example, content which is unacceptable regardless of the criminal law consequences; this includes, for example, content in which children or young people are depicted in unnaturally sexualised postures (JMStV § 4 (1) no. 9. On the other hand, providers of content harmful to children and young people must ensure that children and young people are generally unable to perceive the content (JMStV § 5 (1) no. 1). Intentional or negligent distribution of illegal content and intentional or negligent violation of the age rating are punishable as administrative offences by a fine of up to EUR 500 000. The NetzDG, on the other hand, explicitly targets operators of social networks. As mentioned above, the offences to be reported include the distribution, acquisition and possession of child pornography (StGB § 184b) and threats to life, sexual autonomy, physical integrity or personal liberty (StGB § 241).⁵²

51 Telemediengesetz vom 26.02.2007 (BGBl. I S. 179, 251; 2021 I S. 1380), das zuletzt durch Artikel 3 des Gesetzes vom 12.08.2021 (BGBl. I S. 3544) geändert worden ist.

52 Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23. p. 10–11.

4. Prevention

There are many ways to take preventive measures against cyberbullying within the family or in the school environment. Through role-playing, projects and active media work, children and young people can be sensitised to the problem. Important topics such as data security and the data economy, copyright and privacy rights of oneself and others, rules of online behaviour (netiquette), privacy and the health, social and legal consequences of cyberbullying can and should be discussed. On the one hand, the aim is to develop the confidence to use online media responsibly and competently. On the other hand, to communicate clear boundaries of digital communication.⁵³ To achieve this goal, there are several initiatives in Germany.

As part of the JIM Study 2022, young people were also asked if they had ever been contacted by strangers about cybergrooming on the internet. The term ‘grooming’ refers to the approach and preparation of sexual harassment online with the aim of sexual abuse. A quarter of young people say they have been confronted with cybergrooming, girls more often than boys (girls: 28%, boys: 21%). High school students are more likely to say they have been contacted by strangers. However, nine per cent of young people chose ‘don’t know’, so the number of unreported cases may be much higher.⁵⁴

JUUUPORT is a national online counselling platform for young people who have problems online. JUUUPORT members are volunteer teenagers and young adults from all over Germany who help their peers confidentially with online problems such as cyberbullying, media addiction, sexual harassment, data theft and many more. The advice is privacy-appropriate and free of charge. In addition to counselling, JUUUPORT also carries out active awareness-raising and prevention work. The website provides comprehensive guides and news on current online issues and threats. JUUUPORT’s workers appear in the press and at events and organise awareness-raising campaigns on social media (in particular Instagram, TikTok and YouTube), sensitising their peers to problematic content and interaction risks on the internet, and providing concrete tips for confident, reflective and critical use of digital media. The volunteers are supported by a permanent team of media educators, psychologists, editors, press officers and

53 <https://www.lmz-bw.de/medienbildung/themen-von-a-bis-f/cybermobbing/praevention-und-intervention#:~:text=Rollplaying%2C%20Workshops%20and%20active%20media%20work,f%3%BCr%20to%20raise%20awareness%20of%20the%20problems>

54 Medienpädagogischer Forschungsverbund Südwest JIM-Studie 2022. p. 56–57. https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2022_Web_final.pdf

administrative staff.⁵⁵ In addition, JUUUPORT is organising a national online counselling platform action day, on which it is making it its mission to raise awareness of the problem of cyberbullying.⁵⁶

The Klicksafe is the European Union's awareness-raising centre in Germany, coordinated by the Media Authority of Rhineland-Palatinate and implemented in cooperation with the Media Authority of North Rhine-Westphalia. The Klicksafe has also been coordinating the Safer Internet Centre DE since 2008, which includes the internet hotlines, eco, FSM and jugendschutz.net, as well as the helpline Nummer gegen Kummer. Klicksafe is funded by the European Union's Digital Europe Programme (DIGITAL). The independent information portal www.klicksafe.de provides users with a wealth of up-to-date information, practical tips and useful material on digital services and issues. Its activities also include the implementation of comprehensive campaigns and the development of national certification schemes for teachers and professionals. They also support training for children, young people, parents, teachers and professionals on the opportunities and risks of the Internet. The Klicksafe also networks initiatives and stakeholders in Germany and across Europe to promote media literacy on the Internet.⁵⁷

jugendschutz.net was founded in 1997. They currently operate as a joint federal and state competence centre for the protection of children and young people online. They analyse the Internet in terms of the dangers for children and young people. They focus on issues such as self-harm, political extremism, sexual violence, harassment and cyberbullying. They also investigate services that contain cost traps, present inappropriate advertising or violate the privacy rights of minors. When they receive reports through their online reporting form, they will also examine and assess the content and review the precautions taken by online gaming services and services such as Instagram, YouTube and TikTok to protect against risks and harm. This includes, for example, settings that prevent strangers from contacting unsolicited. Reporting systems are also tested. These should not only be easy to find and simple to use but should also lead to the rapid deletion of breaches. If a website is found to be in breach of the Interstate Treaty on the protection of personal data (JMStV), the service provider or a voluntary self-regulatory organisation is contacted and a request is made to have the infringement stopped. If this does not happen, the matter is

55 See: <https://www.juuuport.de/ueber-uns>

56 See: <https://www.juuuport.de/aktionstag-gegen-cybermobbing>. Materials available at: <https://www.klicksafe.de/cybermobbing/handlungsansatz-zur-praevention-und-intervention-von-cybermobbing>

57 See: <https://www.klicksafe.de/die-initiative>

usually referred to the Commission for the Protection of Minors in the Media (Kommission für Jugendmedienschutz, KJM). If there is a risk to life or depictions of sexual violence against children, the police authorities, such as the Federal Criminal Police Office (Bundeskriminalamt), are immediately involved. The Federal Centre for the Protection of Children and Young People (Bundeszentrale für Kinder- und Jugendmedienschutz, BzKJ) is informed. Their reports and briefings provide in-depth insights into specific problems and highlight the need for action. They also present their findings at conferences and workshops and contribute to the debate on contemporary youth media protection.⁵⁸

The Landesmedienzentrum Baden-Württemberg, together with the #RespektBW project and the 'Bitte Was?! Kontern gegen Fake und Hass' (Countering Fake and Hate) information campaign, it sends a clear signal against online fake and hate. The aim of the campaign is to motivate children and young people to behave respectfully online and thus stand up for good social coexistence. Such projects could result in an informative classroom bulletin board, a self-made film, a code of conduct or even a play on cyberbullying. In this context, 'experts' such as student media mentors, mediators and anti-bullying officers can also be trained. They can provide competent support in acute cases of bullying. In addition, teachers should receive regular training in mediation and conflict resolution.⁵⁹

Examples of mediation as a process of constructive conflict resolution, in which impartial third parties act as mediators to assist in mobbing and cyberbullying cases, can be found in the state of Hessen.⁶⁰

One site, [klicksafe.de](https://www.klicksafe.de), offers manuals on the subject, and one of them describes the decision levels. The school management is responsible for running of the school, intervenes in conflicts in a regulatory way, decides on the convening and composition of the Systemic Conflict Management (SKM) team, leads it, hears parents, victims, perpetrators and their families, decides on educational and disciplinary measures in an administrative act, in a regulatory role, advises victims, offenders and their families. The class teacher is responsible for class management, informs parents of all events affecting them, decides on educational measures outside the administrative act, makes contact offers, in a regulatory role, advises victims, offenders and their families. They

58 See: <https://www.jugendschutz.net/ueber-uns/was-wir-tun>

59 See: <https://www.lmz-bw.de/medienbildung/themen-von-a-bis-f/cybermobbing/praevention-und-intervention#:~:text=Rollplaying%2C%20Workshops%20and%20active%20media%20work,f%C3%BCr%20to%20raise%20awareness%20of%20the%20problems>

60 See: <http://www.schulmediation-hessen.de/index.html>

are the decision-makers. The systemic conflict management professional prepares team meetings and decisions, makes conflict diagnoses, proposes conflict assessments, proposes action strategies, advises team members, evaluates the process, gives feedback if agreements and procedural standards are not respected, takes over documentation. Conflict support professionals conduct interviews with conflict support seekers or confrontation interviews with the accused for social training and harassment intervention or mediation, social training and systemic harassment and brief interventions, advice on mediation of values in the classroom, coaching victims, perpetrators and their parents, triangle meetings, mediation in front of the classes if necessary. Counselling and training professionals (e.g. media education specialists) advise the team and its members on all professional issues.⁶¹

Summary

In conclusion, the prosecution of hate crime is a matter of the state's duty to protect, rooted in fundamental rights. The focus is on the protection of human dignity (Article 1 GG) and the fight against discrimination (Article 3(3) GG). In view of the ultima ratio nature of state punishment, the need for a criminal law provision can only be confirmed in rare exceptional cases. The protection of bodily integrity or the right to social esteem, which is rooted in general rights of personality, is already adequately guaranteed by criminal law. Therefore, the legislator is under no constitutional obligation to extend protection against hate crime by law.

In some cases, hate crime is understood to mean only violent crime. This may be related to the fact that the main focus of statistical surveys or criminological studies is often on hate crimes motivated by right-wing extremism. However, the general social dimension of hate crime goes beyond violent acts motivated by right-wing extremist attitudes. Criminal law is essentially neutral and covers acts irrespective of the ideology of the perpetrator. Any motivation based on certain characteristics of the victim can lead to classification as a hate crime. It is not only people who hold extremist views who can be considered as perpetrators, because such a narrow perspective can result in 'ordinary' manifestations of prejudice and attacks going unnoticed and therefore unaddressed. The perception of the victim is crucial in determining whether a crime is a hate crime.

61 Chapter5_Systemic_Conflict_Management.pdf (klicksafe.de)

A hate crime can be the subject of any offence under the Criminal Code if the offence is committed because of the specific motivation of the perpetrator. With regard to offences criminalising bias-based violence, in addition to classic violent crimes such as homicide, assault and sexual offences, any other offence involving harming or threatening people, such as arson, coercion, robbery, extortion or hostage-taking, may be covered.

Section 192a of the StGB deals with hate-mongering insult, which was newly introduced into the German Criminal Code in September 2021. Its purpose is to close the gap that previously existed in criminal liability for sending hateful content to the persons concerned.

Only the offence of stalking (StGB § 238) explicitly mentions telecommunication – which includes digital forms of communication – as a possible means of committing the offence (StGB § 238 (1) no. 2). Thus, there is an indirect reference to online space as a ‘place of commission’, but it does not follow from the wording of the offence that it is committed exclusively online, only that harassment can be committed online.

An audit of social network deletion practices carried out by jugendschutz.net in January/February 2017 showed that user complaints about hate crime are still not being processed promptly and adequately. YouTube now deletes criminal content 90% of the time. In contrast, Facebook deletes content only 39% of the time and Twitter only 1% of the time. Social network providers have a responsibility to fulfil. Given that existing tools and voluntary commitments promised by social networks are not effective enough and that there are significant problems with the enforcement of applicable law, compliance rules for social networks are needed to effectively and promptly tackle online hate crime.

The criminal law protection of minors against sexual violence on the internet follows from the criminal law provisions on the protection of sexual self-determination (StGB §§ 174-184), whereas in the case of cyberbullying, as mentioned, several criminal law provisions can be applied, such as insult (StGB § 185). In addition to the criminal law provisions, the German Youth Protection Act (JuSchG), the Interstate Treaty on the Protection of Minors in the Media (JMStV) and the Act on the Improvement of Law Enforcement in Social Networks (NetzDG) contain provisions on the protection of minors on the Internet.

There are many ways to take preventive measures against cyberbullying within the family or in the school environment. One is to develop the confidence to use online media responsibly and competently. On the other hand, clear boundaries of digital communication need to be communicated. To achieve this goal, there are several initiatives in Germany.

Bibliography

- Bannenberg, B. Coester, M. and Marks, E. (2004) 'Primary prevention of violence against group members – especially young people. Results of a task force. Part 1', *Forum Kriminalpraevention*, 2(4), pp. 30–36.
- Bannenberg, B. Coester, M. and Marks, E. (2005) (eds) *Kommunale Kriminalprävention, Ausgewählte Beiträge des 9. Deutschen Präventionstages*, Forum-Verlag Godesberg: Mönchengladbach.
- Cyberkriminalität' Strafrechtliche Regelungen in Deutschland und ausgewählten EU-Mitgliedstaaten, Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 039/19,
- Gesetz betreffend das Urheberrecht an Werken der bildenden Künste und der Photographie in der im Bundesgesetzblatt Teil III.
- Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz – NetzDG) vom 1. September 2017 (BGBl. I S. 3352) <https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html>. § (3)
- Glet, A. (2011) *Sozialkonstruktion und strafrechtliche Verfolgung von Hasskriminalität in Deutschland. Eine empirische Untersuchung polizeilicher und justizieller Definitions- und Selektionsprozesse bei der Bearbeitung vorurteilsmotivierter Straftaten. Schriftenreihe des Max-Planck-Instituts für ausländisches und internationales Strafrecht*, Band K154. Berlin: Duncker & Humblot.
- Grundzüge der Beleidigungsdelikte (§§ 185 ff. StGB) aus straf- und zivilrechtlicher Sicht. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 052/22.
- Handlungsansatz zur Prävention und Intervention von Cybermobbing. Vom Mobbing zum Cybermobbing. <https://www.klicksafe.de/cybermobbing/handlungsansatz-zur-praevention-und-intervention-von-cybermobbing>
- https://www.klicksafe.de/fileadmin/cms/download/Sonstiges/Themen/Cybermobbing/Kapitel2_Vom_Mobbing_zum_CyberMobbing.pdf
- International Convention on the Elimination of All Forms of Racial Discrimination, adopted in New York on 21 December 1965
- International Convention on the Prevention and Punishment of the Crime of Genocide, adopted on 9 December 1948
- Jugendschutzgesetz vom 23.07.2002 (BGBl. I S. 2730), das zuletzt durch Artikel 1 des Gesetzes vom 09.04.2021 (BGBl. I S. 742)
- Kugelman, D. (2015) *Möglichkeiten effektiver Strafverfolgung bei Hasskriminalität. Rechtsgutachten*, Berlin: Antidiskriminierungsstelle des Bundes.
- Medienpädagogischer Forschungsverbund Südwest JIM-Studie 2022. pp. 56–57. https://www.mpfs.de/fileadmin/files/Studien/JIM/2022/JIM_2022_Web_final.pdf

- Nussbaum, Maximilian (2021) 'Jenseits der Beleidigung unter Kollektivbezeichnung? – Überlegungen zur Verhetzenden Beleidigung gem. § 192a StGB' *KriPoZ*, 6, pp. 335–342.
- Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Umsetzung von Empfehlungen des NSU Untersuchungsausschusses des Deutschen Bundestage. RefE 2014-04-15 Umsetzung NSU-UA Empfehlungen (bundesgerichtshof.de)
- Referentenentwurf des Bundesministeriums der Justiz und für Verbraucherschutz Entwurf eines Gesetzes zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken, https://netzpolitik.org/wp-upload/2017/03/1703014_NetzwerkDurchsetzungsG.pdf
- Schneider, H. J. (2001) *Kriminologie für das 21. Jahrhundert: Schwerpunkte der internationalen Kriminologie*. Münster: LIT Verlag.
- Schneider, H. J. (2003), 'Hasskriminalität: eine neue kriminologische Deliktskategorie', *Juristen Zeitung*, (58) pp. 497–504.
- Schutz Minderjähriger im Internet durch das Strafrecht Untertitel: Einzelfragen zur Rechtslage Schutz Minderjähriger im Internet durch das Strafrecht Einzelfragen zur Rechtslage. Wissenschaftliche Dienste Sachstand WD 7 – 3000 – 023/23.
- Staatsvertrag über den Schutz der Menschenwürde und den Jugendschutz in Rundfunk und Telemedien (Jugendmedienschutz-Staatsvertrag – JMStV) vom 13.09.2002, zuletzt geändert durch Artikel 2 des Zweiten Medienänderungsstaatsvertrages vom 14./27.12.2021 als Anlage des Gesetzes vom 31.03.2022)
- Verordnung (EU) 2022/2065 des Europäischen Parlaments und des Rates vom 19. Oktober 2022 über einen Binnenmarkt für digitale Dienste und zur Änderung der Richtlinie 2000/31/EG, (Gesetz über digitale Dienste, Digital Services Act, DAS)
- Zakariás, K. (2012) 'Az emberi méltóság a Grundgesetz-ben', *Jogtudományi Közlöny*, (4), pp. 184–192.
- Zakariás, K. (2014) 'Az emberi méltóság védelme az 'Auschwitz-hazugság'-gal szemben a német Szövetségi Alkotmánybíróság gyakorlatában', *Acta Humana*, 2(1), pp. 97–115.
- Internet sources:
- Chapter5_Systemic_Conflict_Management.pdf (klicksafe.de)
- Hate crime | European Union Agency for Fundamental Rights (europa.eu)
- <http://www.schulmediation-hessen.de/index.html>
- [https://www.bidt.digital/glossar/cyberkriminalitaet/#:~:text=Deutschland%20hat%20als%20eines%20der,Daten%20\(%C2%A7%20202a%20StGB\).](https://www.bidt.digital/glossar/cyberkriminalitaet/#:~:text=Deutschland%20hat%20als%20eines%20der,Daten%20(%C2%A7%20202a%20StGB).)

<https://www.eff.org/de/deeplinks/2022/05/platform-liability-trends-around-globe-recent-noteworthy-developments>
<https://www.jugendschutz.net/ueber-uns/was-wir-tun>
<https://www.juuuport.de/aktionstag-gegen-cybermobbing>
Materials available at: <https://www.klicksafe.de/cybermobbing/handlungsansatz-zur-praevention-und-intervention-von-cybermobbing>
<https://www.juuuport.de/ueber-uns>
<https://www.klicksafe.de/die-initiative>
<https://www.lmz-bw.de/medienbildung/themen-von-a-bis-f/cybermobbing/praevention-und-intervention#:~:text=Rollplaying%2C%20Workshops%20and%20active%20media%20work,f%C3%BCr%20to%20raise%20awareness%20of%20the%20problems.>
<https://www.lmz-bw.de/medienbildung/themen-von-a-bis-f/cybermobbing/praevention-und-intervention#:~:text=Rollplaying%2C%20Workshops%20and%20active%20media%20work,f%C3%BCr%20to%20raise%20awareness%20of%20the%20problems>

XIII. DENMARK – FUTURE-PROOF PROVISIONS IN THE FIGHT AGAINST CYBERBULLYING

ZOLTÁN NÉMETH

1. Regulatory issues of hate speech

In Denmark, hate speech¹ is prohibited by law and is officially defined as public statements that threaten, insult or degrade a group based on characteristics such as nationality, ethnicity, religion or sexual orientation.

Anyone who threatens anyone with the commission of a crime in such a way that it is capable of instilling serious fear in the threatened person – regarding his life and physical integrity – shall be punished with a fine or imprisonment of up to 2 years.² The Danish Penal Code therefore defines as a conceptual element in connection with hate crimes that it must be capable of inducing serious fear in the person threatened.

In connection with the commission of a hate crime, it is important to emphasize that the law specifically lists the social groups or characteristics in connection with which the crime may be committed:

- (a) so-called race, skin color;
- (b) descent or national or ethnic origin;
- (c) faith;
- (d) sexual orientation.

The Criminal Code contains special provisions in the case of hate crimes committed in public, when it states that statements made in public that are also

¹ Criminal Code (Straffeloven) Available: <https://www.retsinformation.dk/eli/lta/2021/1851>

² Criminal Code § 266.

aimed at inciting acts of violence or vandalism are punishable, as well as³ anyone who makes a statement publicly or with the intention of spreading it more widely, in which a group of people is threatened, insulted or humiliated because of his so-called race, skin color, national or ethnic origin, religion or sexual orientation, shall be punished by a fine or imprisonment of up to 2 years.⁴ Another qualifying circumstance appears in the regulations, which has an impact on judicial practice. This provision states that it must be considered a particularly aggravating circumstance at the time of sentencing if the hate speech is of a propaganda nature.

The provision was introduced into the Criminal Code in 1939, but the provision on sexual orientation was not introduced until 1987. The concept of hate speech is therefore not specifically included in the Criminal Code, but must be interpreted as a collective term for the above types of crimes.⁵ (Direct) discrimination, hate speech and hate crimes can be seen as three sides of the same thing in the sense that each crime is motivated by prejudice against a particular group. However, the concepts raise different kinds of legal issues, so it is important to distinguish between the concepts.⁶

Denmark has detailed statistics on hate crimes, compiled by the police and publicly available. Based on the data, it can be established that in the period between 2016 and 2020, 2,273 crimes were registered that correspond to the concept of hate crime,⁷ but these were not further broken down, so it cannot be determined exactly how many of these crimes specifically involved hate speech.

Year	Number of cases
2020	635
2019	469
2018	449
2017	446
2016	274

Table 7. Number of hate crimes in Denmark 2016-2020⁸

3 Criminal Code § 266 a.

4 Criminal Code § 266 b.

5 Garly-Nour, 2011, p. 19.

6 Dilou Jacobsen-Kierkegaard, 2008, pp. 99–100.

7 ODIHR Hate Crime Reporting; available at: <https://hatecrime.osce.org/denmark>

8 The table is edited by the author. Source: ODIHR Hate Crime Reporting; available at: <https://hatecrime.osce.org/denmark>

In Denmark, hate speech regulations were tightened between 2016 and 2020, as the government aimed to protect social cohesion and reduce online harassment, as well as racial or religious discrimination. The new regulations placed greater emphasis on defining hate speech and addressing the consequences of such expressions.

Key Changes in Regulation:

- (a) 2016 Enhancements: The first significant change involved broadening the criminal liability for hate speech. Existing laws increasingly targeted online platforms, placing greater responsibility on social media providers to remove hate-inciting content.⁹
- (b) 2018 Reforms: The regulatory framework further expanded with new rules aimed at curbing hate speech based on race, religion, and gender. Increased oversight of online platforms and expedited judicial processes were also included among the measures.¹⁰
- (c) 2020 Amendments: In 2020, additional amendments strengthened sanctions on hate speech. Measures to protect victims also expanded, and new protocols were introduced for handling police reports related to hate speech incidents.¹¹

Statistics showed that the number of hate speech-related crimes initially increased, especially following the 2018 reforms. This rise can be partially attributed to the new regulations and increased reporting options, which allowed victims to approach authorities more easily and safely. The increase in cases indicated that people were more aware of reporting hate-motivated expressions, and the police became better equipped to address these incidents.¹²

Following the 2020 enhancements, however, a slight decrease in case numbers was observed, suggesting that the changes in legislation were exerting a greater deterrent effect. The stricter legal sanctions on hate speech and

9 Columbia Global Freedom of Expression. (2016). *Something's Rotten in Denmark: Criminalizing Blasphemy and Hate Speech Law*. Retrieved Available: <https://globalfreedomofexpression.columbia.edu/updates/2016/02/somethings-rotten-denmark-criminalizing-blasphemy-hate-speech-law/>

10 Council of Europe. (2018). *6th ECRI Report on Denmark*. Available: <https://rm.coe.int/6th-ecri-report-on-denmark/1680a6d5e4>

11 United Nations Office of the High Commissioner for Human Rights. (2021). *Experts of the Committee on the Elimination of Racial Discrimination Ask Denmark about Hate Speech and Hate Crime*. Available: from <https://www.ohchr.org/en/press-releases/2021/11/experts-committee-elimination-racial-discrimination-ask-denmark-about>

12 Danish Institute for Human Rights. (2017). *Hate Speech in the Public Online Debate*. Available: from https://www.humanrights.dk/files/media/migrated/hate_speech_in_the_public_online_debate_eng_2017.pdf

preventive measures gradually contributed to reducing the number of related crimes.¹³

Overall, the tightening of Denmark's hate speech regulations initially led to an increase in crime reports due to higher reporting, but eventually showed a declining trend as stricter sanctions took effect.

However, based on police statistics, it can be determined in what cases and how many times the so-called hate crimes were committed in 2020. The most typical cases are:

- (a) Racist and xenophobic motivation;
- (b) Anti-Semitic background;
- (c) Anti-Muslim hate speech;
- (d) Anti-Christian hate speech;
- (e) Other hate crimes based on religion or belief;
- (f) Anti-LGBT hate speech.

Type of crime	Number of cases in 2020
Racist and xenophobic motivation	360
Anti-Semitic background	79
Anti-Muslim hate speech	87
Anti-Christian hate speech	25
Other hate crimes based on religion or belief	3
Anti-LGBT hate speech	79

Table 8. Number of hate speech crimes in Denmark in 2020¹⁴

In 2020, the Danish Ministry of Justice published a report on the victimization survey between 2005 and 2019. The survey included questions about hate crimes and found, among other things, that 4,300 to 5,800 people were victims of racist violence each year, and 1,500 to 2,500 people were victims of violence because of their sexual orientation. Additionally, in 2019, almost six percent of victims of violence responded that the perpetrator may have been motivated by their gender identity.¹⁵

13 OSCE Hate Crime Reporting. (2021). *Denmark: Hate Crime Data*. Available: from <https://hatecrime.osce.org/denmark>

14 The table is edited by the author. Source: ODIHR Hate Crime Reporting; available at: <https://hatecrime.osce.org/denmark>

15 Exposure to violence and other forms of crime. Victim surveys 2005-2020. (2020) Ministry of Justice Research Office, National Police, University of Copenhagen, Crime Prevention Council [Online]. Available: <https://www.justitsministeriet.dk/>

Of course, a distinction must be made between crimes committed offline and online, and the previously mentioned report of the Danish Ministry of Justice contains a comprehensive survey in this regard as well, so we can get an answer to the question of how the number of hate speech-related crimes is developing in Denmark and what kind of crimes they are. They happen for a reason and which age groups and social groups are most at risk.

During the victim surveys that have been taking place since 2008, they tried to shed light on the extent to which the violence can be classified as a hate crime, e.g. a crime motivated by hatred of a group to which the victim belongs or is believed to belong. The question therefore arises to what extent the violence is motivated by either racism or the victim's (presumed) sexual orientation, according to the victim. As of 2019, the extent to which the violence is motivated by the victim's (presumed) gender identity will also be measured. And from 2020, an additional question will be the extent to which violence is motivated by the victim's religious beliefs. Hate crimes can take other forms, such as politically motivated violence, but these forms were not asked about in the survey.¹⁶ In 2020, 21% of violent incidents involving victims were clearly hate crimes motivated by one or more of the above-mentioned forms of (perceived) group affiliation, corresponding to an estimated number of between 8,300 and 15,100 people.¹⁷

2008 and 2020, eight percent of the victims stated that, in their opinion, the incident was motivated by racism. This means that 4,600-6,000 people between the ages of 16 and 74 are exposed to racially motivated violence each year. The calculations are currently based on few observations, so the results should be treated with considerable caution.¹⁸ In the case of racially motivated violence, a statistically significantly higher proportion of men fell victim than women, and the 25-74 age group is more at risk than the 16-24 year olds.

Violent crimes that are believed to be motivated by the victim's sexual orientation or gender identity are less common than crimes motivated by racism. In the case of four percent of the victims of violence in the period between 2008 and 2020, it can be proven that the act of violence was definitely motivated by the victim's (presumed) sexual orientation or gender identity. This means that between 1,900 and 2,900 people between the ages of 16 and 74 are subjected to violence because of their sexual orientation or gender identity every year. There

wp-content/uploads/2021/12/Udsathed-for-vold-og-andre-former-for-kriminalitet.-Offerundersogelserne-2005-2020-WT.pdf (hereinafter: Victim surveys 2005-2020).

¹⁶ Victim surveys 2005-2020. p. 78.

¹⁷ Victim surveys 2005-2020. p. 79.

¹⁸ Victim surveys 2005-2020. p. 79.

is no statistically significant difference between the number of women and men who believe that the violent episode was definitely motivated by the sexual orientation of the victim.¹⁹

Regarding violence due to religious beliefs, it can be stated that almost 11 percent of victims are involved. The calculations here are based solely on a one-year study and very few observations, and are therefore subject to considerable uncertainty.²⁰

The Department of Justice survey indicates that the alleged religious beliefs of the victim are more often behind it than racism, but it is very important to note that in previous years victim surveys, religion was not asked as a possible motive.

A Department of Justice survey concluded that the willingness of victims of hate crimes to report is neither lower nor higher than the willingness of victims of other types of violence to report (34%).²¹

Of course, hate speech also appears online, and the Danish Ministry of Justice also examined this in its report. Of those who answered that they had been exposed to crimes committed online in 2020, just over a tenth had been exposed to hate speech. The most widespread type of hate speech is racist, followed by discriminatory statements regarding sexual orientation or gender identity, while the smallest category is discriminatory statements related to religion.

In the entire group of victims of crimes committed on the Internet, women and men report their involvement in approximately the same proportion. Among the victims of crimes committed on the Internet, 40-74 year olds are statistically significantly less exposed to hate speech on the Internet than younger age groups,²² which may also be due to the fact that this age group uses the Internet and its various platforms significantly less.

1.1. The relationship between freedom of expression and hate speech

In the context of hate speech, it is worth briefly reviewing where the boundaries of freedom of speech and expression of opinion are drawn in the Danish regulations, since a violation of these boundaries can already lead to committing the act of hate speech. Freedom of expression is not absolute in Denmark either, so it is a crime to make defamatory or invasive statements, and the disclosure or use of confidential information is prohibited. This is subject to the provisions of

¹⁹ Victim surveys 2005-2020. p. 79.

²⁰ Victim surveys 2005-2020. p. 80.

²¹ Victim surveys 2005-2020. p. 80.

²² Victim surveys 2005-2020. p. 142.

the Danish Penal Code, the Danish Public Administration Act and the Danish Trade Secrets Act, and the employee may be subject to special confidentiality obligations based on an agreement (e.g. in the employment contract), so there are several laws in force that set the limits of freedom of speech. Article 77 of the Danish constitution²³ states in general the freedom of expression, which everyone has the right to verbally and in writing, but with liability in court.

Legislation	Restrictive provision
Constitution	Freedom of speech can be exercised while taking responsibility before the court (Article 77)
Penal Code	Defamation (§ 267) and defamation (§ 269)
Public Administration Act ²⁴	Limitation of the right to inspect documents (§ 30)
Trade Secrets Act ²⁵	Unlawful acquisition of trade secrets (§ 4), protection of trade secrets (§ 6)

Table 9. Legal restrictions on freedom of speech in Denmark²⁶

It is widely agreed in Danish legal theory that Article 77 of the constitution protects the so-called ‘formal freedom of speech’ (formel ytringsfrihed), which means that it cannot be required that one’s speech be published or otherwise disseminated submit it for official review.²⁷ However, there is a difference of opinion regarding whether § 77 covers the so-called to ‘material freedom of speech’ (materiel ytringsfrihed), the right not to be punished for one’s own speech. It is agreed that the phrase ‘under the jurisdiction of a court’ gives legislators some power to limit free speech, but conversely, several court decisions suggest that some substantive freedom of speech exists.²⁸ The debate is about whether or not there are limits to material freedom of speech.²⁹

In connection with hate speech, it is worth mentioning two cases that ended in court proceedings in Denmark. Freedom of speech advocate Lars Hedegaard was prosecuted in December 2009 for comments he made criticizing Islam. He was first acquitted in the District Court in January 2011, then convicted on appeal to the Supreme Court in May 2011, and finally acquitted in April 2012 by the Danish Supreme Court, which ruled that it could not be proven that he made

²³ Danish Constitution (LOV nr 169 af 05/06/1953 – Danmarks Riges Grundlov) Article 77.

²⁴ Public Administration Act (Lov om obnøghed i forvaltningen – LOV nr 606 af 12/06/2013) § 30.

²⁵ The Law on Business Secrets.

²⁶ Edited by the author.

²⁷ Zahle, 2006, p. 536.

²⁸ Zahle, 2006, p. 539.

²⁹ Zahle, 2006, pp. 539–552. He.

the statements intentionally.³⁰ In another interesting case, Danish politician Jesper Langballe pleaded guilty and was convicted of hate speech based on a newspaper article he wrote in connection with Hedegaard's case about sexual violence in Muslim families.³¹

1.2. Findings

The Danish legislation prohibits hate speech, which is officially defined as public statements that threaten, insult or degrade a group based on characteristics such as nationality, ethnicity, religion or sexual orientation. Hate speech is usually motivated by racist and xenophobic motives, anti-Semitic background, anti-Muslim hate speech, anti-Christian hate speech, hate speech based on religion or belief, and anti-LGBT hate speech. The Criminal Code, the Public Administration Act and the Business Secrets Act also contain provisions regarding these acts. These laws also limit freedom of speech in the Danish legal system.

2. Regulation of cyberbullying

2.1. Cybercrime in general in Denmark

Cybercrime is a collective term for crimes committed with the help of computers and networks, most often the Internet.³² Crimes traditionally covered by this term include:

- (a) hacking;
- (b) industrial espionage;
- (c) distribution of information systems codes;
- (d) electronic counterfeiting;
- (e) data fraud;
- (f) electronic payment crimes;
- (g) computer crimes.

30 Pia Buhl Andersen (2012). Lars Hedegaard was acquitted in a trial over his remarks about Muslims [Online]. Available: www.politiken.dk

31 Jesper Langballe settles defamation over Muslim rape comments (2010) [Online]. Available: <https://www.icenews.is>

32 Feldtmann, 2019, p. 6.

There is no fixed definition of the term, but it can be divided into two categories:³³

- (a) Advanced cybercrime (or high-tech crime) – sophisticated attacks against computer hardware and software;
- (b) Cyber-enabled crime – Traditional crime (crimes against children, financial crimes and terrorism) has taken a new turn with the advent of the Internet.

Slightly simplified, the difference between the two categories is that the computer and network belonging to the first category is the target of the attack, while the computer or network belonging to the second category is the means of the attack.

2.2. Danish regulation of cyberbullying

One of the goals of this country chapter is to present Danish regulations in the field of cyberbullying. There are many different laws and regulations governing violence and threats as well as digital harassment in Denmark. These are the following:

- (a) Working Environment Act;³⁴
- (b) Various guidelines of the Danish Working Environment Protection Authority;
- (c) Criminal Code;
- (d) Personal Data Act;
- (e) the so-called the ‘respect package’ created by the Danish Ministry of Justice.

It can therefore be seen that internet harassment and cyberbullying are present in various segments of society and unfortunately affect several social strata. It can be related to crime, school bullying, workplace abuse, but it is also present in the lives of public administration workers, and it can also be important in terms of the protection of personal data. Despite the fact that cyber-threats and harassment in the online space do not basically look back on a significant past, this is offset by its almost unhindered progress due to the rapid development of the Internet and digital devices.

³³ INTERPOL website: <https://www.interpol.int/Crime-areas/Cybercrime/Cybercrime>

³⁴ Working Environment Act (Bekendtgørelse af lov om arbejdsmiljø) Available: <https://www.retsinformation.dk/eli/lta/1995/184>

The various Danish laws therefore contain scattered provisions regarding online bullying, but they nevertheless form a system and respond to various types of acts.

Legislation	Provision on cyberbullying
Working Environment Act	Separate chapter: rules on offensive acts, including harassment and sexual harassment § 22 – organization of work § 23 – unlawful acts
Criminal Code	§ 119 a) – harassment of employees in the public service § 264 d) – protection of privacy § 266 – threat § 266 b) – racism or discrimination clause § 267 – defamation
Personal Data Act	Management of personal data
Act on occupational accident insurance	§ 6 – the consequences of online harassment are also considered a workplace accident

Table 10. Indirect appearance of cyberbullying in Danish legislation³⁵

2.3. Cyberbullying in the workplace

According to Danish occupational health and safety legislation, digital bullying is an abusive act that can have the same health consequences as other abusive acts. Harassment is an umbrella term for bullying, sexual harassment and other forms of workplace wrongdoing, including when it occurs digitally.

The Act on the Working Environment makes a distinction between abusive acts being committed within the workplace or by an external person who is not part of the workplace. The Danish Working Environment Authority³⁶ also handles digital harassment based on who is perpetrating it.³⁷ Based on this, the following categories are distinguished in the guide they prepared:³⁸

- (a) Offensive acts within the workplace between employees or between employees and managers;
- (b) According to the Danish Working Environment Authority, abusive actions in the form of digital harassment by external parties such as parents,

³⁵ Edited by the author.

³⁶ Website of the Working Environment Authority (Arbejdstilsynet): <https://at.dk>

³⁷ Arbejdstilsynet (AT) guidance on workplace abuse. [Online]. Available: <https://at.dk/regler/at-vejledninger/kraenkende-handlinger-4-3-1/>

³⁸ Arbejdstilsynet (AT) guidance on workplace abuse. [Online]. Available: <https://at.dk/regler/at-vejledninger/kraenkende-handlinger-4-3-1/>

pupils, students, users, patients, customers or relatives are considered violence.

Whether digital bullying takes place within the workplace or is perpetrated by individuals outside the workplace, it is a workplace issue that the workplace has a duty to prevent and address – both during and outside of work hours.

According to the guide, offensive work-related acts can include:

- (a) Preservation and withholding of necessary information;
- (b) hurtful comments;
- (c) unjustified withdrawal or reduction of duties and responsibilities;
- (d) defamation or exclusion from the professional community;
- (e) attacks or criticisms affecting the privacy of employees;
- (f) shouting;
- (g) physical attacks or threats thereof;
- (h) hostility;
- (i) offensive written messages, text messages, images and videos, including on social media;
- (j) abusive phone calls;
- (k) scoff;
- (l) workplace exploitation.

Under workplace legislation, work at all stages must be designed, organized and carried out in such a way that it is completely safe in the short and long term in relation to offending acts. This means that abuses must not harm the safety or health of employees in the short or long term, and the employer must take effective measures to ensure that the physical or mental health of employees does not deteriorate.³⁹

The guide also analyzes in detail the root causes of online or offline bullying at work. Research shows that there are many reasons for acts of aggression or harassment. According to the Danish analysts, the working conditions of the individual as well as the organizational and management methods contribute to the occurrence of abuses. The same applies to interactions between employees and between employees and managers. These can be, for example:

- (a) Inadequate organization of work, e.g. too high, unclear or contradictory expectations for employees;
- (b) inadequate information and communication;

³⁹ § 22 of the Working Environment Act.

- (c) discrimination;
- (d) lack of constructive problem solving and conflict management;
- (e) workplace management of changes in work (such changes may result in illegal acts if they are not accompanied by adequate information);
- (f) unclear values and behavioral norms in the workplace.

The law on workplace accident insurance,⁴⁰ digital harassment is also considered a workplace accident. The law defines an accident at work as a mental or physical injury caused by an event or impact occurring suddenly or within five days.⁴¹ Violent acts committed by external persons outside the workplace in connection with work are also classified as workplace accidents. This also applies to threats and harassment that are carried out digitally, e.g. on social media sites or by e-mail, within and outside of working hours, if they can be linked to work. An offensive act in the form of digital harassment, which occurs between employees or between managers and employees within the workplace, if it causes personal injury, is also considered an occupational accident. Such workplace accidents must be reported and registered in the same way as other workplace accidents. Most workplaces have an accident registration and reporting system that can be used and applied where appropriate.

2.4. Cyberbullying rules in the Danish Criminal Code

The Criminal Code sets various limits on the freedom of expression and these provisions apply to the online space as well, without specifically naming cyberbullying and cyberbullying. Cybercrime, on the other hand, already has a separate status in the Danish criminal code. The presentation of the following provisions of the criminal code is important because they are mostly related to the topic of cyberbullying:

- (a) § 119 a) – harassment of public service employees;
- (b) § 264 – protection of privacy;
- (c) Section 266 – threat;
- (d) § 266 b) – racism or discrimination clause;
- (e) § 267 – defamation.

⁴⁰ Act on workplace accident insurance (Bekendtgørelse af lov om arbejdsskadesikring – LBK nr 376 af 31/03/2020).

⁴¹ § 6 of the Workplace Accident Insurance Act.

2.4.1. *Harassment of civil servants*

Pursuant to § 119 of the Criminal Code, harassment of persons working in the public service is a crime and is punishable by up to eight years of imprisonment since the tightening in 2019.

According to the law, a person who, by means of force or threats, obstructs someone who is responsible for a public service activity with the aim of preventing or obstructing such person from performing a lawful act of service, or forcing him to perform an act of service.

The announcement issued by the Danish Attorney General on the matter clarifies the concept of public service and includes persons employed in public administration (i.e. state, regional and local government institutions) as well as other persons acting in the scope of public service duties, including, for example, politicians. In addition, depending on the circumstances, employees of private companies who, based on an agreement, perform tasks on behalf of the public sector may also belong to this group.⁴²

2.4.2. *Privacy protection*

A fine or imprisonment of up to six months is punishable by a fine or imprisonment of up to six months for anyone who publishes a call, picture, or other recording of another person's private life without their authorization. The crime can also be committed online. The international dimension of the Internet affects the degree of application of national law. The 9a. §, the penal code received a future-proof provision stating when there is Danish criminal authority in relation to violations of the law when text, audio or visual material is made generally available via the Internet. § 9 limits the application of the principle of effect, so when publishing materials on the Internet, the laws of all countries do not have to be followed, but they fall under Danish jurisdiction.⁴³

2.4.3. *Threat*

Based on the provisions of the Criminal Code, the prospect of a serious disadvantage that is capable of inducing serious fear in the person threatened, especially if the threat is directed against life and physical integrity, is punishable

⁴² Announcement of the Chief Prosecutor: Harassment, threats and violence against public employees (Section 119, 119a and 121) (§ 119, § 119 a og § 121) – CIR1H 10246, 19.12.2019] Available: <https://www.retsinformation.dk/eli/retsinfo/2019/10246>

⁴³ Jensen, 2010.

by a fine or imprisonment of up to 2 years. According to the provision, the threat must be capable of creating serious fear for the life, health or well-being of the person at risk or others. Whether a threat is suitable for instilling fear always depends on the specific assessment of the given case. Several points may be relevant here, e.g. the tone of voice between the parties. It is very important that the threat itself must be capable of causing serious fear.

2.4.4. Discrimination Clause

It can also be done online, the so-called a crime described in the racism or discrimination clause, according to which a person makes a statement publicly or with the intention of spreading it more widely, in which a group of people is discriminated against on the basis of race, so-called color, national or ethnic origin, religious or offends because of his sexual orientation, is punishable by a fine or imprisonment of up to 2 years. When imposing a penalty, it should be considered a particularly aggravating circumstance if the offense involves propaganda.

2.4.5. Defamation

Section 267 of the Danish Criminal Code provides for the crime of defamation, when it states that anyone who insults another's honor by word or deed in such a way as to reduce the victim's esteem as a citizen, shall be punished with a fine or imprisonment of up to 4 months. Not only in Denmark, but also in other countries, it is a clear trend that defamation is increasingly appearing in the online space as well. Overall, it can be said that, in the opinion of the Criminal Law Council, especially in the light of technological development, there is a risk that defamation will spread quickly and widely on the Internet, and consequently there is a greater risk of increasing harmful effects. The fact that defamation, as a clear starting point – and according to the proposal of the Criminal Law Council continues to be – is the subject of private prosecution, and because of this very rarely proceedings are initiated, in the opinion of the Council, cannot in itself mean that it is not sufficient grounds for criminal law defense.⁴⁴

According to the Criminal Law Council, it is not necessary for the individual defamation itself to be particularly serious, but as a whole it must be a

44 Report of the Criminal Law Council on Breach of the Peace and Honor, No. 1563. report. [Online]. Available at: <https://www.justitsministeriet.dk/sites/default/files/media/Pressemessagender/pdf/2017/bet1563.pdf>

defamatory statement that is capable of causing another person a particularly serious violation.⁴⁵

According to the interpretation of the Criminal Law Council, § 267 of the Criminal Code covers defamation with defamatory words or actions, as well as spreading false accusations. There is agreement in the legal literature that the wording of the provision is somewhat vague, but nevertheless covers both the making and dissemination of disparaging statements.⁴⁶

2.5. Protection of personal data and its relation to cyberbullying

The Personal Data Processing Act⁴⁷ is the main legislation governing when and how personal data can be processed. The most common breach of the Privacy Act occurs when images or videos are posted on social media, websites and blogs. The publication of images of recognizable persons on the Internet is considered electronic processing of personal data, but there are no special rules in the Personal Data Act regarding the publication of images on the Internet without consent. According to the Danish data protection agency, which supervises the law on personal data,⁴⁸ whether an image or video is infringing always depends on a specific assessment, since the infringement is usually realized by publishing them.

2.6. Prevalence of online bullying in Danish educational institutions

“I define bullying or victimization in the following general way: A student is being bullied or victimized when he or she is exposed, repeatedly and over time, to negative actions on the part of one or more other students. It is a negative action when someone intentionally inflicts, or attempts to inflict, injury or discomfort upon another – basically what is implied in the definition of aggressive behavior.”⁴⁹

According to Danish national legislation, schools must formulate anti-bullying strategies to ensure that the educational environment promotes the child’s

45 Report of the Criminal Law Council on Breach of the Peace and Honor, No. 1563. report, p. 149.

46 Report of the Criminal Law Council on Breach of the Peace and Honor, No. 1563. report, p. 153.

47 Act on the processing of personal data (Lov om behandling af personlige data – LOV nr 429 af 31/05/2000).

48 Website of the Danish Data Protection Agency: <https://www.datatilsynet.dk>

49 Olweus, D (1994) Bullying at school: basic facts and effects of a school based intervention program. *Journal of Child Psychology and Psychiatry* 35: pp. 1171–1190.

well-being and the achievement of the highest possible level of development and learning. Government policy includes a three-year assessment of the school environment, including the physical, mental and aesthetic aspects of that environment, a description and evaluation of its problems, and an action plan to address them.⁵⁰

The following quote from a student perhaps best illustrates what bullying means to a student, whether online or offline:

“The teacher showed us a sheet of paper and said we could spit on it, stamp it, crumple it – but not tear it. Then he asked us to try to straighten it again, but it was impossible to smooth out all the creases.”⁵¹

Danish research proves that there is a significant connection between bullying and subsequent crimes. Studies show that bullying is a risk factor for later crime. Therefore, limiting school and Internet bullying is an important crime prevention effort. According to the research, those young people who are most exposed to digital bullying are those for whom the following factors are true:

- (a) dissatisfaction;
- (b) social exclusion;
- (c) loneliness;
- (d) little self-confidence;
- (e) self-destructive behavior.

Analyzing the risk factors further, the researchers highlighted that in addition to the above factors, there are also risk-increasing characteristics. Statistics show that children living in poorer families and those raised in children’s homes are at greater risk than their peers. Another important finding is that the victims of offline bullying are generally exposed to a greater risk, so when preventing offline bullying, you must also be aware of the online dimension of bullying. A 2018 survey of 1,390 9th grade students found that 37% of youth who had been bullied online had also bullied others on digital media in the past year.

The research also revealed the reasons behind online bullying. Young people who commit online bullying indicated the following reasons:

50 Background paper on protecting children from bullying and cyberbullying, Expert Consultation on protecting children from bullying and cyberbullying, 2016. Firenze, p. 22. Available at: https://violenceagainstchildren.un.org/sites/violenceagainstchildren.un.org/files/expert_consultations/bullying_and_cyberbullying/background_paper_expert_consultation_9-10_may.pdf

51 Background paper on protecting children from bullying and cyberbullying, Expert Consultation on protecting children from bullying and cyberbullying, 2016. Florence, p. 1.

- (a) was angry with the victim (40%);
- (b) do not know the reason (15%);
- (c) the person he bullied also bullied someone else (14%);
- (d) the person he bullied did not fit into the community (9%);
- (e) thought it would make him popular (4%);
- (f) he was afraid that he too would be bullied (2%);
- (g) he was also bullied (9%);
- (h) other reason (9%).

This 2018 survey by the National Institute of Public Health provides an insightful overview of the prevalence of digital bullying among Danish students aged 11, 13, and 15. The statistics reveal several key trends:

- (a) **Prevalence of Victimization:** Younger students, particularly 11-year-olds, report the highest rates of online bullying, with 10-11% experiencing it. Among 13-year-olds, girls are more frequently bullied online (12%) compared to boys (8%). By age 15, online bullying decreases slightly, with 7-8% experiencing bullying.
- (b) **Perpetration of Bullying:** Across all age groups, boys are more likely to bully others online than girls. 11-year-old boys (7%) are more likely to bully others online compared to girls (4%). Among 13-year-olds, boys again have a higher bullying rate (10%) than girls (6%). This trend intensifies by age 15, where 11% of boys have bullied others online compared to 4% of girls.
- (c) **Trends by Age:** The likelihood of being bullied online seems to decrease slightly with age, but the rates of boys bullying others increase as they get older. This could indicate that older boys, particularly by age 15, may be more prone to engage in online bullying, while younger students, regardless of gender, are more vulnerable to being targeted.
- (d) **Gender Differences in Bullying Behavior:** Girls experience a slightly higher rate of victimization than boys at age 13, suggesting possible gender-based differences in the type or frequency of online bullying. Boys, however, consistently show higher rates of perpetration across all ages, which may highlight different social dynamics or behaviors among male and female students.

Overall, the survey highlights the persistence of digital bullying among young people, particularly the gendered and age-related differences in both experiencing and perpetrating online bullying. This data may suggest the need for targeted interventions, especially aimed at reducing boys' involvement in bullying

as perpetrators and providing support to younger students who are more frequently victimized.⁵²

It can therefore be seen that a significant part of the interviewed students have already been involved in school online or offline bullying on some site, and this will probably increase in the future with the unstoppable spread of the Internet, which will most likely be followed by legislation.

2.7. Remarks

Cyberbullying and crimes committed in the online space are carving out an ever-increasing share of Danish crime, so their regulation is becoming more and more important today. However, the Danish legislation does not name the situation of internet harassment or intimidation, but orders the provisions of the criminal code to be applied to crimes in the online space as well, i.e. for example the crime of defamation can be committed both online and offline and there is no difference between them in terms of punishment. Online bullying itself is present both in the world of work and in the school environment and outside of it, and predominantly affects the younger age group.

3. Regulation and practice related to prevention

3.1. Prevention in schools

Safer Internet use can support the effort to ensure that as few minors as possible are on the victim side or on the perpetrator side. For this purpose, the Safer Internet Center was established in Denmark.⁵³ The Safer Internet Center in Denmark, as a knowledge center and mediator of the latest developments in the field of the use of online technologies by children and young people, has established extensive cooperation with representatives of academic institutions, industry, government agencies and law enforcement agencies. The center has a network and an advisory board representing a wide range of stakeholders. The Center consists of three organizations:

⁵² Rasmussen–Kierkegaard–Vork Rosenwein–Holstein–Trab Damsgaard–Due, 2018, pp. 1–20. He.

⁵³ Safer Internet Center (Sikker Internet Center Danmark) website: <https://sikkertinternet.dk/english>

- (a) Media Council for Children and Youth:⁵⁴ an awareness-raising center whose main task is to provide information and educate on the safer and more positive use of online technologies;
- (b) Save the Children Denmark:⁵⁵ acts as a hotline where anyone can report online child abuse;
- (c) Center for Digital Youth Care:⁵⁶ a helpline that offers online counseling to all children and young people in Denmark.

In Denmark, there is therefore a complex system that helps both students and parents. The former in creating a safer internet use for them, while the latter in being able to protect their child. The Media Council for Children and Youth can provide parents, students and schools with a lot of resources, consisting of training and information materials as well as events and programs.

In Denmark, in addition to the above system, the National Complaints Board against Bullying was established to prevent and deal with online and offline bullying at school,⁵⁷ which provides assistance to institutions, students and parents alike. The Complaints Board evaluates the legal environment and established good practices in an annual report. Significant changes took place in the field of school bullying in 2017, when the so-called Anti-harassment Regulation, which introduced the following changes:

- a) All primary and secondary schools should have an anti-bullying strategy, including a digital anti-bullying strategy, which must be published;
- b) All primary and secondary schools, if they experience bullying or bullying-like incidents, must prepare and implement an action plan to combat bullying;
- c) The National Anti-Bullying Complaint Board was established, to which students and parents can complain in the event of inadequate or missing anti-bullying strategies and action plans of institutions;
- d) Mediation activities conducted by the Danish Education and Quality Agency (Styrelsen for Undervisning og Kvalitet, hereinafter: STUK) have been established, with the help of which mediation is offered for the purpose of reconciling the parties.⁵⁸

54 Website of the Media Council for Children and Youth: <https://www.medieraadet.dk>

55 Save the Children Denmark website: <https://redbarnet.dk>

56 Center for Digital Youth Care website: <https://cfdp.dk/cfdp-english/>

57 Den Nationale Klageinstans mod Mobning website: <https://dcum.dk/forside/nkmm>

58 National Appeals Council's assessment of anti-harassment provisions (2020) [Online]. Available at: <https://dcum.dk/media/3662/200831-evaluating-af-antimobbetbestlemeter-og-den-nationale-klageinstans-mod-mobning.pdf>

Regarding the system operating in Denmark, it is perhaps worth emphasizing that the fundamental goal is to restore peace between the parties, and for this purpose a special mediation procedure⁵⁹ was introduced, the procedure of which is also specifically regulated. The mediation process gives the parties an opportunity to talk together about what happened and see if they can agree on possible ways to work together for the student's well-being. The participants of the meeting are the persons involved in the conflict and their companions. Participation in mediation is voluntary for all parties. The student's well-being is the focus point of the mediation process, so the student's perspective also plays an important role in the meetings. The student's point of view is either brought to the meeting by a mediator, or in the case of young people, they are offered to participate in the meetings themselves. Mediation counselors lead the meetings and ask questions that help the parties clarify their own points of view and listen to others' points of view. Mediation consultants do not take a position during the mediation, and the solution is worked out by the parties.⁶⁰ The process of the mediation procedure consists of several steps:

- (a) Mediation decision: Danish Center for Educational Environment (Dansk Center for Undervisningsmiljø, hereinafter: DCUM) will judge the case. If the case is deemed suitable for mediation during the processing of the case, the institution and the complainants are offered mediation. From 2018 to the beginning of 2020, mediation was offered in a total of 24 cases, of which the parties said yes in 12 cases (9 have been conducted so far).
- (b) If both parties agree to the mediation, STUK will contact them and provide information about the mediation.
- (c) The first mediation meeting is held: At the meeting, the mediation advisors facilitate the discussion. The primary purpose of the first meeting is for the parties to discuss what happened and listen to each other's points of view. In some cases, the parties can start discussing common solutions at the first meeting. Two consultants from STUK evaluate the discussion and, based on this, develop a proposal for the next mediation meeting. STUK conducted mediation in 9 cases in 2018 and 2019, in 6 of which a mediation meeting was held.
- (d) A second mediation meeting will take place: The aim of the second mediation meeting is for the parties to examine possible ways of cooperation

59 Executive order on the processing of complaints related to harassment and the like addressed to the Danish Education Center (Bekendtgørelse om behandling af klager til Dansk Center for Undervisningsmiljø om mobning og sylke BEK nr 255 af 06/04/2018) § 7 Available at: <https://www.retsinformation.dk/eli/lta/2018/255>

60 Evaluation of the National Appeals Council regarding anti-harassment provisions, p. 88.

based on the well-being of the students, and based on this to develop joint agreements and solutions. According to STUK, a breakthrough can happen here, to which the first meeting also contributed.

- (e) A learning meeting can be held at the end of the process, the purpose of which is to make use of the experience from the case, to see what general lessons can be learned from it in the school and the municipality. They choose which focus areas they think STUK can help them with – it can be about conflict tools or more information about bullying, the investigation of bullying.⁶¹

In Denmark, mediation, specifically through the Victim-Offender Mediation (VOM) program, can be utilized at various stages of the criminal justice process. This program facilitates a constructive dialogue between the victim and the offender, aiming to address the aftermath of the crime. Participation is entirely voluntary for both parties.

The mediation process can be initiated at different points:

- (a) Pre-Trial Stage: Before formal charges are filed, mediation can be considered as an alternative approach to address the conflict arising from the offense.
- (b) During Prosecution: While the case is under prosecution, mediation may be pursued alongside the legal proceedings, providing an opportunity for reconciliation without interfering with the judicial process.
- (c) Post-Conviction: After a conviction, mediation can serve as a restorative measure, helping to repair the harm caused and potentially aiding in the offender's rehabilitation.

It's important to note that engaging in mediation does not replace the legal proceedings or any imposed penalties. Instead, it serves as a supplementary process that can offer emotional closure and mutual understanding for both the victim and the offender.⁶²

3.2. Findings

In the Danish system, great emphasis is placed on the prevention of cyberbullying and other forms of harassment and threats. Specific guidelines and

⁶¹ Assessment of the National Board of Appeals regarding anti-harassment provisions, pp. 89–90. He.

⁶² Danish National Police. (n.d.). *Victim-Offender Mediation (VOM) in Denmark*. Available: from <https://politi.dk/en/law-and-information/victimoffendermediation>.

training are available for employers and employees, while an extensive network helps students and their parents of educational institutions to find the right solution and, even if concrete prevention has not succeeded, at least the harmful consequences can be mitigated, even with the help of a mediation process.

4. Responsibility of service providers and institutions

4.1. Responsibility of service providers

An analysis and presentation of three of the Danish laws is necessary in order to make the regulation of the responsibility of Internet service providers transparent. The Act on e-commerce,⁶³ the Act on Network and Information Security of Digital Services⁶⁴ and the Network and Information Security Act⁶⁵ contain measures that are similar as the Hungarian legislation.

The law on e-commerce names the cases in which the service provider is exempted from liability:

- (a) if the transfer includes the automatic, intermediate and short-term storage of information, if this storage serves only to complete the transfer and if the storage does not last longer than can reasonably be expected;⁶⁶
- (b) the service provider that transmits the information provided by the user of the service on a communication network is not responsible for the automatic, intermediate and temporary storage of this information, or for the content of the information, if the storage is carried out solely for the purpose of later transmission;⁶⁷
- (c) the service provider is not responsible for the storage of the information or the content of the stored information, if the storage takes place at the request of the service provider providing the information.⁶⁸

63 The E-Commerce Act (E-handelsloven LOV nr 227 af 22/04/2002) Available at: <https://www.retsinformation.dk/eli/lta/2002/227>

64 Act on network and information security of digital services (Bekendtgørelse om net- og informationssikkerhed for visse digitale services, BEK nr 452 af 08/05/2018).

65 Network and Information Security Act (Lov om net- og informationssikkerhed, LOV nr 1567 af 15/12/2015.) Available: <https://www.retsinformation.dk/eli/lta/2015/1567>

66 § 14 of the Act on e-commerce.

67 § 15 of the Act on e-commerce.

68 § 16 of the Act on e-commerce.

The Act on Network and Information Security of Digital Services states that digital service providers identify and take appropriate and proportionate technical and organizational measures to manage risks related to the security of the networks and information systems they use in connection with the digital service.⁶⁹ Providers of digital services are also obliged to notify the Danish Business Authority and the Cybersecurity Center as soon as possible of any event that has significant consequences for the performance of their service.⁷⁰ This notification must be made on a special website organized for this purpose (virk.dk). If the operator does not have all the information for the purpose of the notification available at the time of the notification, the operator issues a partial notification. A partial notification must be followed by a full notification as soon as possible.

4.2. Responsibility of educational institutions

The Danish liability system has three levels. The first authority prescribed by law for many tasks is the municipality responsible for the educational institution.⁷¹ All responsible authorities of primary and secondary education have the following three tasks:

- (a) Preparing and publishing an anti-bullying strategy;
- (b) preparation, implementation of an action plan;
- (c) obligation to take action.

In practice, the authority to process and decide complaints falls on local government administrators, consultants and managers.⁷²

The next authority in the ‘chain of responsibility’ is the DCUM. DCUM is an institution established under the Education Environment Act, whose aim is to help ensure the development of a good teaching environment in Denmark. In relation to anti-harassment regulations, it performs three functions: it helps students, parents and institutions, it carries out development work, it supervises institutions and it also acts as an appeals authority.

The third authority is the STUK, which was given the opportunity to mediate with the entry into force of the relevant executive decree.

69 § 3 of the Act on Network and Information Security of Digital Services.

70 § 4 of the Act on Network and Information Security of Digital Services.

71 Executive order on the processing of complaints related to harassment and the like addressed to the Danish Education Center.

72 Evaluation of the National Appeals Council regarding anti-harassment provisions p. 6.

The primary distinction between DCUM and STUK lies in their roles and scopes within Denmark's educational framework:

- (a) DCUM: This is the Danish Centre for Educational Environment, focusing on promoting and enhancing the quality of learning environments across educational institutions. DCUM develops materials, guidelines, and tools to support schools and educators in creating positive and inclusive educational settings. For instance, they provide templates for developing value sets and anti-bullying strategies in schools.
- (b) STUK: This is the Danish Agency for Education and Quality, operating under the Ministry of Education. STUK is responsible for overseeing and ensuring the quality of education in Denmark. Its functions include developing curricula, conducting assessments, and implementing educational policies to maintain and improve educational standards nationwide.

In each educational institution, the institution's work related to bullying is contained in the anti-bullying strategy, which must be prepared. This should include how the institution deals with bullying when it occurs. If a student, the student's parents, or the school itself experiences bullying, the institution is obliged to immediately activate the action obligation contained in the strategy. This fast action obligation includes the preparation and implementation of a concrete action plan, the transitional measures necessary for the intervention, and information on the content of the action plan. If the student and parents are satisfied with the action plan, the cases can usually be handled properly at the local level, however,⁷³ based on the evaluation of the National Appeals Board, it can be seen that many students and parents find that the institution either does not live up to its obligation to act, or does, but not in a satisfactory way. Perhaps this is also why most parents turn directly to the National Anti-Bullying Complaints Board. DCUM always returns the complaint to the first instance and, in parallel, provides telephone guidance on legal provisions and obligations. If the students or parents do not agree with the municipality's decision, the institution acting in the first instance forwards the case to the National Anti-Harassment Appeals Board. At the National Anti-Bullying Complaint Board, parents, students and the educational institution are offered the possibility of mediation. When the National Bullying Appeals Board makes a decision, it can choose to uphold the local authority's original decision or change it.

73 Evaluation of the National Appeals Council regarding anti-harassment provisions p. 10.

4.3. Responsibility of workplaces

Under workplace legislation, work at all stages must be designed, organized and carried out in such a way that it is completely safe in the short and long term in relation to offending acts. This means that abuses must not harm the safety or health of employees in the short or long term, and the employer must take effective measures to ensure that the physical or mental health of employees does not deteriorate.⁷⁴ The work environment law therefore classifies the responsibility of the employer to protect its employees from online harassment, and they can also employ appropriate consultants and provide special training for employees. Pursuant to the law, if the employer does not have the necessary expertise to carry out safety and health protection training and consulting within the company, the employer must request external expert assistance in order to ensure that the working environment of the employees is always completely safe. The Minister of Employment can establish more detailed rules in this regard⁷⁵ and specifically define the forms and frameworks of using consultants.⁷⁶

4.4. Remarks

While preventing cyberbullying is key question, it is equally important to properly address online bullying that has already occurred. Part of this is, on the one hand, the responsibility of service providers for the content they provide, and on the other hand, the responsibility of educational institutions and workplaces is also of prime importance. In the Danish education system, there is a multi-level institutional system for parents, students and educational institutions to find appropriate solutions and deal with problems appropriately. It can be stated that the appropriate treatment can be considered a form of prevention in the long term, as it educates the actors involved in the cases, draws their attention to how parents can protect their children or how educational institutions should handle the situations that have arisen. The same is true for workplaces, as Danish legislation makes it the responsibility of employers to create a suitable and healthy working environment and, in parallel, to train employees. However, in the case of educational institutions and workplaces, it can be stated that the regulations of our country could still be expanded and improved, and it may be especially worthwhile to consider strengthening the dialogue between the stakeholders in the field of prevention and treatment.

⁷⁴ § 22 of the Working Environment Act.

⁷⁵ § 12 of the Working Environment Act.

⁷⁶ § 13 of the Working Environment Act.

Summary

Danish legislation prohibits hate speech, which is officially defined as public statements that threaten, insult or degrade a group based on characteristics such as nationality, ethnicity, religion or sexual orientation. Hate speech is usually motivated by racist and xenophobic motives, anti-Semitic background, anti-Muslim hate speech, anti-Christian hate speech, hate speech based on religion or belief, and anti-LGBT hate speech, and the Criminal Code, the Public Administration Act and the Business Secrets Act also contain provisions regarding these acts, which laws also represent the limits of freedom of speech in the Danish legal system.

Cyberbullying and crimes committed in the online space are taking an ever larger share of Danish crime, so their regulation is becoming more and more important today. However, the Danish legislation does not name the situation of internet harassment or intimidation, but orders the provisions of the criminal code to be applied to crimes in the online space as well, i.e. for example the crime of defamation can be committed both online and offline and there is no difference between them in terms of punishment. Online bullying itself is present in the world of work and in the school environment and predominantly affects the younger age group.

In the Danish system, great emphasis is placed on its prevention. Specific guidelines are available to employers and employees, while an extensive network helps students and their parents of educational institutions to find the right solution and, even if concrete prevention has not succeeded, at least the harmful consequences can be mitigated, for example by means of a mediation process, which is effective and all procedural form validating the aspect of the person concerned.

Preventing cyberbullying is very important, but it is equally important to properly address online bullying that has already occurred. Part of this is, on the one hand, the responsibility of service providers for the content they provide, and on the other hand, the responsibility of educational institutions and workplaces. In the Danish education system, a multi-level institutional system is available to parents, students and educational institutions to find appropriate solutions and deal with problems. It can be stated that the appropriate treatment can be considered a form of prevention in the long term, as it educates the actors involved in the cases, draws their attention to how parents can protect their children or how educational institutions should handle the situations that have arisen. The same is true for workplaces, as Danish legislation makes it the responsibility of employers to create a suitable and healthy working environment and, in parallel, to train employees.

Regulating cyberbullying and online crimes in Denmark, or anywhere, involves balancing freedom of speech, privacy, and the safety of individuals in the digital space. Here are a few regulatory ideas that could enhance protection against these types of crimes:

- (a) **Stricter Accountability Measures for Online Platforms:** Legislation could require social media platforms and digital communication services to take greater responsibility for moderating harmful content. This might involve mandatory reporting mechanisms for users, faster content removal protocols, and transparency about platform policies and enforcement practices.
- (b) **Mandatory Age Verification Systems:** To protect minors from cyberbullying and predatory behavior, regulations could require age verification mechanisms for users on platforms popular with younger audiences. These systems, while respecting privacy, would help shield children from inappropriate content and potential cyberbullying interactions.
- (c) **Increased Penalties and Criminalization:** Strengthening the criminal code to include severe penalties for cyberbullying, stalking, and other online crimes can deter individuals from engaging in these harmful behaviors. Denmark could look to establish specific cyber harassment laws that include fines, mandatory education, or community service programs focused on rehabilitation and awareness.
- (d) **Anonymous Reporting Systems:** Establishing anonymous reporting channels for victims of online bullying and harassment encourages individuals to come forward without fear of retaliation. Authorities could coordinate these reports to identify repeat offenders across platforms.
- (e) **Educational Initiatives and Public Awareness Campaigns:** Education plays a crucial role in preventing online crimes. Mandatory digital literacy education in schools and public awareness campaigns could promote responsible online behavior, helping users recognize and report abusive behavior while protecting their personal information.
- (f) **Specialized Cybercrime Units and Training:** Funding and training specialized law enforcement units to handle cyberbullying and online crimes can help address these issues more effectively. These units would need up-to-date resources and training to track, investigate, and prosecute cases within digital contexts.
- (g) **Cross-Border Legal Cooperation:** Cybercrimes often span borders, making cross-border cooperation essential. Strengthening collaboration between Danish law enforcement and international organizations (such as Europol) could improve Denmark's ability to prosecute offenders from outside the country.

- (h) Research and Data Collection: Gathering data on cyberbullying and online crime trends helps policymakers make informed decisions. Denmark could establish research bodies to monitor and analyze data trends, providing insights to guide future regulatory approaches.

By implementing a mix of preventative, educational, and punitive measures, Denmark could create a safer online environment, addressing the rise in cyberbullying and digital crimes effectively.

Bibliography

- Gary Andersen, L., Nour, S. (2011) 'Hate Crimes in Denmark – The Path to Effective Protection', Report No. 8. Danish Institute for Human Rights
- Dilou Jacobsen, B., Kierkegaard, A. (2008) *Rapport om auskuppet af discrimination og hadforbrydser i Københavns Kommune* (Report on the extent of discrimination and hate crimes in the city of Copenhagen), Institute for Human Rights
- Zahle, H. (2006) *Danmarks Riges Grundlov med kommentarer* (Commentary on the Constitution of the Kingdom of Denmark), 2nd edition, Copenhagen: Jurist og Økonomforbundets Forlag
- Feldtmann, B. (2019) *The Danish Criminal Code section 263(1) – An analysis of the Danish safeguard against hacking*. Aalborg University
- Rasmussen, M., Kierkegaard, L., Vork Rosenwein, S., Holstein, B., Trab Damsgaard, M., Due, P. (2018) *Statens Institut for Folkesundhed*; https://www.sdu.dk/da/sif/rapporter/2019/skoleboernsundersoegelsen_2018
- Jensen, ITB (2010) *Privatlivsbrænkelser på interneten* (Infringement of privacy on the Internet) Rettid; <https://law.au.dk/fileadmin/Jura/dokumenter/forskning/Rettid/2010/afh8-2010.pdf>
- OLWEUS, D (1994) Bullying at school: basic facts and effects of a school based intervention program. *Journal of Child Psychology and Psychiatry* 35: pp. 1171–1190.

XIV. FINLAND: WHERE PREVENTION STARTS IN SCHOOLS

ZOLTÁN NÉMETH

1. Hate speech regulation issues

1.1. The hate speech

Hate speech is a global phenomenon. In various countries, there is a growing social awareness of hate speech and its effects on society, relations between different population groups and social cohesion. The trends and methods of hate speech do not stop at national borders, and the forms of hate speech certainly have one thing in common: they all violate the right to human dignity, personal integrity, security, honor, equality and non-discrimination.

Hate speech (*Vihapuhe*) has been a heated topic in Finnish jurisprudence for some time, and its precise definition remains debated to this day. When defining the concept of hate speech, the recommendation of the Council of Europe can serve as a basis, but it is not used as a reference in Finland. According to the recommendation, hate speech refers to all forms of expression that spread, incite, promote, or justify racial hatred, xenophobia, anti-Semitism, or other forms of hatred based on intolerance, including expressed intolerance, aggressive nationalism and ethnocentrism, as well as discrimination and hostility towards minorities, migrants, and people of immigrant origin.¹

Hate speech goes beyond specific hate speech defined as a crime, speech that violates human dignity, which² is also regulated in the Constitution of

¹ General Policy Recommendation No. 15 on combating hate speech, adopted by the European Commission against Racism and Intolerance (ECRI) in December 2015. available at: <https://rm.coe.int/ecri-general-%20policy-recommendation-no-15-on-combating-hate-speech/16808b5b01>

² Article 1 (2) of the Constitution of Finland.

Finland and is prohibited by the prohibition of discrimination, or sexual harassment and gender-based harassment prohibited by the Equality Act. Hate speech is the use of words that are intended to exclude a particular group from the community and make people of that group suspect, untrustworthy, or inferior. They may even claim that they are a security threat to society and the majority population. Hate speech is not mutual and is not intended to convey facts or justify the claims made. In hate speech, the facts are distorted and certain groups and individuals are presented as enemies.³

When we look for the constitutional foundations of the prohibition of hate speech, it can be seen during the analysis of the Finnish constitution that it also contains specific measures that try to prevent hate speech from a constitutional point of view. The constitution ensures the inviolability of human dignity, individual rights and freedoms, and promotes justice in society,⁴ and states that no one can be discriminated against without reasonable cause on the basis of sex, age, origin, language, religion, belief, opinion, health, disadvantage or due to another reason arising from his person.⁵

However, hate speech as such is not considered an independent crime under Finnish law. However, hate speech is considered a crime under the Finnish Criminal Code⁶ if the crime committed contains the the basic characteristics of hate speech. The most common of such actions are the following:

- (a) incitement and its more serious cases⁷ (the purpose of classifying incitement as a crime in the Criminal Code is to protect groups defined on the basis of their skin color, birth situation, national or ethnic origin, religion or belief);
- (b) and violation of the sanctity of religion⁸ (one who publicly blasphemes God, or publicly slanders or despises what a church or religious community⁹ otherwise considers sacred in accordance with the Freedom of Religion Act, or who disrupts worship, other religious practices or funerals by shouting or threatening behavior) disturbs);

3 Hallamaa, 2019. 47(8). [Online] Available at: https://helda.helsinki.fi/bitstream/handle/10138/311966/191106P_iivi_R_s_sen_vihapuheprosessi_uskonnollis_politsikalena_performanssina.pdf?sequence=1

4 Article 1 (2) of the Constitution.

5 Article 6 (2) of the Constitution of Finland.

6 Penal Code (Rikoslaki – 19.12.1889/39). [Online]. Available: <https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001#L11>

7 Criminal Code Chapter 10 § 10a.

8 Criminal Code Chapter 17 § 10.

9 Act on Freedom of Religion (Uskonnonvapauslaki 6.6.2003/453 .) [Online]. Available: <https://www.finlex.fi/fi/laki/ajantasa/2003/20030453>

- (c) the provisions on defamation¹⁰ or threat may apply;¹¹
- (d) in relation to hate speech, the provisions of public incitement to commit a crime¹², dissemination of information that violates the right to privacy¹³ or stalking.

If the hate speech contains the essential elements of the above crimes, it is considered a hate crime, which can be a crime against an individual, group, institution or their representative. Such crimes can have numerous motivations because of the victim's perceived or real ethnic or national background, religious beliefs, worldview, sexual orientation, gender identity or disability. A discriminatory motive (as the offender's motivating factor) can serve as a basis for increasing the punishment.¹⁴

Aiding and abetting the commission of hate crimes are punishable acts under the Finnish penal code. Punishment goes beyond direct aiding and abetting: for example, according to the law, racist organizations are classified as organized criminal groups, and participation in their activities is punishable. However, for instance, the Pohjoismaiden Vastarintaliike was disbanded because it was a racist organization, which was based on the law on associations.

There may also be cases where hate speech does not contain the essential elements of a violation of law, which are prerequisites for criminal liability, but it is classified as harassment under the Act on the Prohibition of Discrimination and is therefore illegal.¹⁵ This means an intentional or actual violation of a person's dignity, if the behavior creates a humiliating, intimidating, hostile or offensive mood or atmosphere towards the person due to their origin, disability or sexual orientation.

The Act on Equality between Women and Men¹⁶ prohibits sexual harassment¹⁷ and gender-based harassment.¹⁸ Sexual harassment is verbal, non-verbal or physical unwanted behavior that intentionally harms a person's mental or physical integrity or creates an intimidating, hostile, humiliating or offensive

10 Criminal Code, Chapter 24, Sections 9-10. §.

11 Criminal Code Chapter 25 § 7.

12 Criminal Code Chapter 17 § 1.

13 Criminal Code, Chapter 24, Section 8 and Section 8a.

14 Penal Code, Chapter 6, Section 5, Paragraphs (1).

15 Law on the Prohibition of Discrimination (Yhdenvertaisuuslaki, 1325/2014.) [Online]. Available at: <https://www.finlex.fi/fi/laki/alkup/2014/20141325> , Section 14.

16 The law on equality between women and men (Laki naisten ja miesten silesestä tasa-arvosta 609/1986.), available: <https://finlex.fi/fi/laki/ajantasa/1986/19860609>

17 Section 7 (7) of the Act on Equality between Women and Men.

18 Section 7 (8) of the Act on Equality between Women and Men.

atmosphere. Gender-based harassment refers to unwanted behavior that is not sexual in nature, but is related to a person's gender or gender identity and with which this person's mental or physical integrity is intentionally violated or an intimidating, hostile, humiliating or offensive atmosphere is created.

The table below shows the Finnish legal provisions that can be linked to legal norms prohibiting or punishing hate speech.

Legislation	Related provision
Constitution	Article 1 (2) – Human dignity Article 6 (2) – Prohibition of discrimination
Penal Code	Chapter 11 § 10a – agitation Chapter 17 § 10 – violation of the sanctity of religion Chapter 24 Chapters 9–10 § – defamation Chapter 25 § 7 – threat Chapter 17 § 1 – public incitement Chapter 24 §§ 8 and 8a – dissemination of information violating personal privacy Chapter 12 § 2 – incitement to war
Law on Prohibition of Discrimination	Section 14 – Harassment
Law on Equality between Women and Men	§ 7 (7) – sexual harassment § 7 (8) – gender-based harassment

Table 11. Hate speech provisions in Finnish legislation¹⁹

1.2. The limits of freedom of expression in the context of hate crimes

Freedom of expression must always be taken into account when deciding whether an act should be considered hate speech. Freedom of speech and expression are key fundamental human rights. The Finnish constitution guarantees everyone this right when it states that everyone has the right to freedom of expression, which includes the expression, distribution and reception of information, opinions or other communications without prior hindrance.²⁰ However, the Finnish constitution regulates the detailed rules related to freedom of expression in a separate law,²¹ i.e. there is no unlimited freedom of expression in Finland either. The main restrictions on freedom of speech that are referred to in the Constitution of Finland arise from the Criminal code. Expression of opinion is therefore not an absolute right, as it has been restricted by national legislation,

¹⁹ Edited by the author.

²⁰ Article 12 (1) of the Constitution.

²¹ Law on the use of freedom of expression in the mass media (Laki sananvapauden kövämistä joukviestinnässä, 13.6.2003/460), available at: <https://www.finlex.fi/fi/laki/ajantasa/2003/20030460>

in particular to protect other fundamental rights. These rights include non-discrimination, equality, freedom of religion, freedom of conscience and the right to personal security.²²

In colloquial terms, the term hate speech is often used to refer to messages containing prejudice against certain groups or other similar opinions. Such expressions can be harmful and unpleasant, but they cannot always be prohibited, as they fall under the scope of freedom of expression.²³ In Finland, there is a great way to express this concept. Hate speech is literally translated as ‘vihapuhe’ and this is the correct Finnish term. (Viha = hate, Puhe = speech.) We also have the term ‘vihainen puhe’, which means ‘angry speech’. They say: “Vihainen puhe is not always vihapuhe”. (Angry speech is not always hate speech.)

The punishment of hate speech restricts freedom of expression as it seeks to exclude certain groups and individuals from public life.. In Finland, in addition to certain population groups and individuals, hate speech and threats are increasingly directed against representatives of professional groups, such as journalists, researchers, police officers, prosecutors, judges and human rights defenders, which negatively affects the protection of human rights. Hate speech against the police, prosecutors and courts can be extremely serious from the point of view of the rule of law.²⁴

In one case, in May 2012, a trial was started for inciting an ethnic group and six people were convicted.²⁵ Another public debate about hate speech in the spring of 2012 related to blog posts by a member of parliament in 2008, in which he said he had “tested the limits of free speech” with his views on Islam. The lower courts rejected the charge of incitement against the ethnic group, but the Supreme Court convicted the representative in June 2012, who was then forced to resign.²⁶

It is also worth noting the following regarding the restriction of freedom of expression. There are several reasons why the rules on restricting freedom of expression must be clear. It is important to know what kind of criticism is allowed, but it is also necessary to avoid creating a chilling effect on public debate. Everyone should have the opportunity to make critical remarks without

22 Words Are Actions More Efficient Measures against Hate Speech and Cyberbullying, 2019, p. 18. He.

23 Words Are Actions More Efficient Measures against Hate Speech and Cyberbullying, 2019, p. 18.

24 Words Are Actions More Efficient Measures against Hate Speech and Cyberbullying, 2019, p. 19.

25 Pöyhtäri-Haara-Raittila, 2013, pp. 17–25.

26 Pöyhtäri-Haara-Raittila, 2013, pp. 17–25. He.

fearing that others will send hateful messages in response, leading to accusations of online shaming. Since it is difficult to draw a clear line between an expression that intentionally initiates shaming and one that merely criticizes something or someone, it is not possible to criminalize the initiation of online shaming. Similarly, everyone should have the opportunity to make critical remarks without the fear of being accused of participating in a shaming action, even if they are unaware of such an action.²⁷

1.3. Statistics

Finland regularly reports data on hate crimes to the ODIHR. Data on hate crimes are collected by the Finnish Police University Research Department, the Ministry of the Interior, the Prosecutor's Office, the Finnish Ministry of Justice and the Ministry of Statistics. Finland regularly conducts victimization surveys to assess unreported hate crimes.²⁸

Year	Hate crimes recorded by the police	Punishable	Convicted
2020	1177	48	42
2019	900	22	17
2018	880	55	21
2017	1497	63	37

Table 12. Number of hate crimes in Finland²⁹

The victim report prepared by the Finnish Ministry of Justice³⁰ provides accurate statistics on how the number of hate crimes developed in the period 2014-2018. The report reveals that verbal abuse was committed in a significant number of cases, but physical abuse and discrimination are common, as well as crimes against property and property (usually religiously motivated) and defamation occur in smaller numbers. The report also examined the root causes of

27 Perspectives on Platform Regulation : Concepts and Models of Social Media Governance Across the Globe – <https://helda.helsinki.fi/server/api/core/bitstreams/ce499b09-fea8-4e25-a846-3e222f937552/content>, p 485.

28 ODIHR hate crime reporting, [Online]. Available: https://hatecrime-osce-org.translate.goog/finland?_x_tr_sl=en&_x_tr_tl=hu&_x_tr_hl=hu&_x_tr_pto=sc

29 Edited by the author.

30 Finnish Ministry of Justice Victim Report 2014-2018 [Online]. Available: https://www.riku.fi/content/uploads/su_file/2140__Uhrien_kokemuksia_viharikossita_2014_2018.pdf, p. 10.

hate crimes.³¹ In the background of the majority of hate crimes, there is some kind of racial or ethnic reason, but in many cases there are sexual motives, religious reasons and other gender motives as well.

Little research data is available on the perpetrators of hate speech. The VIPU team at the Helsinki Police Department investigated hate crimes, especially on the Internet. Based on the cases investigated by the group, the perpetrator was mostly a middle-aged man. 98 percent of the people behind the hate speech were over 30 years old, and 85 percent were men. According to the study, those who spread hate speech on the Internet often act in their own name in public.³² The VIPU group recorded the cases it investigated primarily as hate crimes, rarely as extreme crimes. The number of hate crimes in Finland increased in 2018, particularly in cases related to ethnicity, religion, and sexual orientation. The reported crimes were mostly in the form of verbal attacks and harassment, though incidents of physical violence also occurred. A portion of hate crimes remains underreported, and to improve the accuracy of police data, better data collection and increased awareness are necessary.³³

1.4. Preventing hate speech

The spread of hate speech in the world of the Internet is almost unlimited, so it is very important that individual governments try to devote more resources to prevention. In Finland, there are several programs that focus on prevention, and several studies have already been published that research and present new areas of hate speech. Hate speech can be created with many goals and forms of action. The distinction between them is important for the prevention of hate speech.³⁴ The purpose of hate speech can be, for example, to prevent the political participation of certain people, or it can also be a means of influencing individual political decisions.³⁵ For example, it has been observed that extremist movements try to intensify the social debate with offensive speech, and to silence moderate positions with targeted attacks. Intensification of debate can weaken people's willingness to participate in public debates and social activities. The silencing effect can result in certain views and information not being taken into account in decisions. And the result can be a phenomenon that researchers call

³¹ Finnish Ministry of Justice Victim Report 2014-2018, p. 12.

³² Mäkinen, 2019.

³³ Poliisin tietoon tullut viharikollisuus Suomessa 2018 (Hate Crimes Reported to the Police in Finland 2018) – Available: <https://www.theseus.fi/handle/10024/261556>

³⁴ Knuutila–Kosonen–Saresma–Haara–Pöyhtäri, 2019

³⁵ Knuutila–Kosonen–Saresma–Haara–Pöyhtäri, 2019, p. 14.

the spiral of silence: when only those who use inappropriate language speak up, that seems to be the common and only opinion.³⁶ According to Finnish studies, hate speech seems to be the most effective way to silence those who are already in a vulnerable position. Although such messages cannot always be banned, authorities, educational institutions, employers or online platform operators can help promote a culture of discussion in which the number of hate speech-type crimes can be reduced.³⁷ The obligations in this regard are regulated by the anti-discrimination law³⁸, which names three ‘actors’ and defines their tasks:

- (a) authorities;
- (b) training institutions;
- (c) employers.

The law states that the authority has a duty to promote equality. The authority evaluates the realization of equal opportunities in its activities and takes the necessary measures to promote the realization of equality. Preventive measures must be effective, appropriate and proportionate, taking into account the authority’s operating environment, resources and other circumstances. The authority must prepare a plan for the measures necessary to promote equality.

The educational organizer and the educational institution maintained by him must evaluate the realization of equal opportunities in his activities and take the necessary measures to promote the realization of equal opportunities. The measures must be effective, appropriate and proportionate to the educational environment, resources and other circumstances of the institution. The trainer must ensure that the educational institution has a plan of measures necessary to promote equal opportunities. The educational institution and the educational institution it manages must provide students and their guardians, as well as students or their representatives, with the opportunity to be heard.

1.5. Summary

Based on Finnish regulations, hate speech does not have a specific legal status, but there is a current legislative effort to increase the punishability of hate speech. During the analysis of the Finnish constitution, it can be seen that it also contains specific measures that try to prevent hate speech even constitutionally. These are provisions on the prohibition of discrimination and the protection of

36 Knuutila–Kosonen–Saresma–Haara–Pöyhtäri, 2019, p. 15.

37 Words Are Actions More Efficient Measures against Hate Speech and Cyberbullying, 2019, p. 18.

38 Law on Prohibition of Discrimination, Sections 5–8. §.

human dignity. Hate speech is fully regulated in the Finnish Criminal Code, it just doesn't use the exact term. , however, it is linked to several crimes depending on whether the motives typical of hate crimes appear during the commission. Based on the available statistical data, it can be seen that the phenomenon is constantly present in the everyday lives of Finnish citizens and is very difficult to limit with the help of the Internet. Therefore, in Finland, many preventive campaigns support this work and the field is continuously researched (the latest such research area is the impact of hate speech on social decision-making). It is important to mention that Finnish legislation is active in this area, as the criminalization of the denial of the Holocaust and other crimes against humanity is clarified by introducing a separate provision in the Criminal Code.³⁹

However, in its 2019 report, ECRI makes several observations regarding Finland, among which the following are worth highlighting:⁴⁰

- (a) The ECRI noted with satisfaction that in 2015, all parliamentary parties once again signed the *European Political Parties Charter for a Non-Racist Society*, and that during the 2017 municipal elections, all major parties—except for the Finns Party—required their candidates to sign a declaration against racism. Despite these commendable steps, however, some political figures continued to make discriminatory remarks.
- (b) Following the arrival of 32,400 asylum seekers to Finland as part of the 2015 European migration crisis, there was an increase in anti-immigrant and anti-Muslim rhetoric in the country. This anti-immigration rhetoric heightened ethnic intolerance and polarization. Some politicians sought to gain votes by exploiting fears over the costs of immigration and the perception that foreigners were overrepresented in crime or posed a threat to national identity. Certain members of the Finns Party, in particular, made Islamophobic comments; for example, in 2016, a Member of Parliament claimed that “all terrorists are Muslims” and called for “the removal of all Muslims from the country”. Additionally, during the 2017 municipal elections, political candidates of immigrant origin faced racist remarks and threats.
- (c) In public places, such as public transport, people who appear different or have a different skin color than the majority population—such as Roma, immigrants (especially Somalis), and those identified as LGBT individuals—often face verbal abuse and insults. A 2016 survey revealed that half of LGBT respondents had been victims of harassment in the past

³⁹ The text of the bill – <https://oikeusministerio.fi/en/project?tunnus=OM191:00/2023>

⁴⁰ ECRI Report Finland (2019) – <https://rm.coe.int/fifth-report-on-finland/1680972fa7>, p. 15–21.

five years. Roma respondents also noted that Roma women, in particular, were frequently subjected to insults, especially when accessing social services, due to their traditional attire.

- (d) A 2018 FRA-EU survey found that 63% of people of African descent in Finland experienced racist harassment in the past five years, the highest rate among the countries surveyed. However, only 30% of these incidents were reported. Prejudice against Black people was also evidenced by incidents involving ‘blackface’; for example, at a 2018 university event, some students appeared in blackface makeup and used racist language.
- (e) ECRI expressed concern over the increasing visibility of Nazi swastikas in public places in recent years. In December 2018, during Finland’s Independence Day, hundreds of anti-immigration protesters marched through the streets of Helsinki, where the police confiscated three Nazi flags and arrested the flag bearers. ECRI welcomed the recent decision by the National Non-Discrimination and Equality Tribunal, which deemed the public display of Nazi symbols as a form of hate speech and found it in violation of the anti-harassment provisions of the Non-Discrimination Act.
- (f) Members of the Sámi community pointed out that racist remarks about them remain prevalent in daily life, particularly during discussions about the Arctic Railway Project. ECRI noted that derogatory comments and prejudice against the Sámi create an atmosphere in which members of the indigenous community feel restricted in expressing their culture, such as wearing traditional clothing or using their language in public spaces.

2. Regulation of cyberbullying

In the context of Finland, when examining the rules related to cyberbullying, it is worthwhile to examine several different areas, since several different rules consist of a fairly mature legal regulation focused on prevention. Some online hate crimes occur in workplaces and educational institutions or in connection with them therefore the relevant provisions can be found in the legislation dealing with the world of work and the field of education.

In many cases, discrimination itself can even lead to online abuse, which is why the Finnish anti-discrimination law contains provisions in this context.⁴¹ The law states a general prohibition of discrimination and victimization,

41 Anti-Discrimination Act Chapter 3 Section 8.

according to which no one can be discriminated against on the basis of age, origin, nationality, language, religion, belief, opinion, political activity, trade union activity, family relationships, health status, disability, sexual orientation or other personal characteristics to distinguish based on. Discrimination is prohibited, regardless of whether it is based on fact or assumption against a person. According to the law, in addition to direct and indirect discrimination, harassment and instructions to discriminate are also considered discrimination. On the other hand, proportionally different treatment, the purpose of which is to promote actual equality, or to prevent or eliminate disadvantages resulting from discrimination, is not considered discrimination. Direct discrimination occurs when a person is treated less favorably on the basis of his or her personal characteristics than another person in a similar situation was or is being treated. According to the anti-discrimination law, there are cases when different treatment can be justified:

- a) differential treatment does not constitute discrimination if the treatment is based on legislation and otherwise has an acceptable purpose and the measures to achieve the purpose are proportionate;
- b) the different treatment has a fundamental and human rights-acceptable purpose, and the measures to achieve the purpose are proportionate.

2.1. Cyberbullying in the Finnish Criminal Code

Finland is one of the 14 EU member states that has a specific definition of cyberbullying⁴² and the Finnish criminal code also contains provisions that can be applied in the case of cyberbullying.⁴³ Cyberbullying can include, for example, insulting the victim on a discussion forum or sending mean, unfounded e-mails to the victim.⁴⁴

Legislation	The crime committed
Criminal Code Section 24 9-10 §	Defamation
Criminal Code Section 25 § 7a	Stalking
Criminal Code Chapter 25 § 7	Threat

Table 13. Crimes related to cyberbullying⁴⁵

42 Dalla Pozza–Di Pietro–Morel–Psaila, 2016, p. 25.

43 McCully, 2019, p. 14.

44 Dalla Pozza–Di Pietro–Morel–Psaila, 2016, p. 167.

45 Edited by the author.

Defamation can be committed both online and offline and refers to cases where false information is untruthfully stated about someone, causing suffering or contempt for the victim. However, defamation can also occur with factual statements, making false information just one possible element..⁴⁶ According to Finnish law, defamation can also be carried out against a dead person. Aggravated, the law regulates the case when the defamation causes particularly great suffering or harm to the victim.⁴⁷

The criminal code punishes the crime of stalking, which can also be committed online.⁴⁸ We can talk about this when someone threatens, follows, observes, contacts or otherwise unlawfully persecutes someone else in a way that causes fear or anxiety in the person being persecuted. Intimate violence and especially termination of the relationship can be related to stalking, which is why stalking has been considered a crime in Finland since 2014. The reason for the criminalization of stalking was that Finland signed the Istanbul Convention (CETS 210) in 2011. The convention stipulates that the signatory countries must ensure that repeated threatening behavior towards others is punishable. Stalking is likely to cause fear and anxiety in the victim. Stalking is usually extremely painful for the victim and sometimes it can feel like the harassment is never ending.

One of the most common forms of cyberbullying is threat⁴⁹ In the case of an illegal threat, it means that the victim is threatened in such a way that they have reason to fear his own safety and property. Threats can be made over the phone, verbally, by e-mail or in writing. Essentially, threats that cause real fear in the victim can be classified here. Threats often include threats of violence or destruction of property.

2.2. Cyberbullying in the workplace

Finland is a typical example of countries that address bullying⁵⁰ (and online bullying) primarily through workplace safety and health legislation. Thus, the Finnish Workplace Protection Act of 2002 contains a separate section on workplace harassment.⁵¹ It is reactive in nature and obligates the employer to act upon becoming aware of it. The section also covers the inappropriate behavior

⁴⁶ Section 24 § 9 of the Criminal Code.

⁴⁷ Criminal Code Section 24 § 10.

⁴⁸ Criminal Code Section 25 7a. §.

⁴⁹ Criminal Code Chapter 25 §7.

⁵⁰ Hoel-Vartia, 2018, p. 47.

⁵¹ Workplace Protection Act (738/2002). Available: <https://www.finlex.fi/en/laki/kaannokset/2002/en20020738.pdf>, section 28.

of third parties, which means that the employer is obliged to take action even if the perpetrator is a third party.

The law also makes it clear⁵² that the employees themselves also have a duty to refrain from harassment. In addition, it contains separate sections on prevention that also apply to harassment, including risk assessment and the employer's general duty of care.

Pursuant to the law, if harassment or other inappropriate treatment of an employee occurs at the workplace and poses a threat to the employee's health, the employer is obliged to take measures with the available means to remedy the situation after becoming aware of it.⁵³ Harassment and cases of inappropriate treatment should be dealt with primarily at the workplace according to the Finnish approach. According to the Occupational Safety and Health Act, employers and employees must work together to maintain and improve workplace safety.

If a workplace's own capacity is not sufficient, occupational health professionals, such as occupational health providers, can provide the necessary support. Occupational health and safety inspectors check compliance with the rules. The occupational safety inspectors of the occupational safety departments supervise compliance with the rules related to harassment and other forms of inappropriate behavior. They prepare a report on their workplace inspections. If necessary, the occupational health and safety department can make a binding decision for the employer.

Of course, when investigating workplace harassment or cyberbullying, it is worth analyzing which cases fall into this category. Under the Act, inappropriate behavior or treatment is any treatment that disrupts work and harms an employee. Mistreatment includes hurtful words, actions and attitudes. Inappropriate behavior and treatment⁵⁴ can also lead to gender-based harassment. Gender-based harassment can be physical or verbal. Insinuations, gestures, nude pictures and harsh language can be just as hurtful as a physical insult. Continuous and unfounded criticism of someone's performance at work, defamation of their reputation, insulting nicknames or isolation from the working community are also considered inappropriate treatment. Continuous and regular harassment and inappropriate treatment can damage or endanger the employee's health. Bullying can cause psychosomatic symptoms, illness and anxiety. The longer the bullying goes on, the harder it is to deal with it.

Prolonged harassment can cause difficulties for the employee and exhaust his physical and mental resources. It may happen that the subject of the

⁵² Section 18 of the Workplace Protection Act.

⁵³ Section 28 of the Workplace Protection Act.

⁵⁴ Law on equality between women and men § 7.

harassment has to take longer sick leave or take an early retirement. Colleagues may fear becoming embroiled in the conflict, causing the subject's social network to collapse.

In connection with workplace harassment, it is worth dealing with gender-based harassment, which includes demeaning or condescending speech about someone's gender, sexual harassment, and actions that cause confusion, fear, pain, and anger. Some examples of sexual harassment are innuendos, sexually charged jokes, and comments about someone's body, clothing, or personal life. Sexual harassment also includes sexually suggestive language, demands, physical contact, rape, and attempted rape.⁵⁵

It is not only harassment that can lead to a crime that can also occur in the workplace. The distribution of information that violates the right to privacy also falls within this scope. In this case, someone who unlawfully disseminates information, hints or images regarding another person's private life using the mass media or otherwise in a way that is accessible to many people, an act that causes harm or suffering to that person.⁵⁶ According to the Criminal Code, the distribution of information, hints or images about the private life of a person in a political, business position or civil servant position, or in a similar position, if it is necessary to reveal a matter important to society, is not considered to be dissemination of information that violates the right to privacy.

The legislation related to workplace cyberbullying is summarized in the following table, in connection with which it is worth highlighting that these acts can be committed both online and offline:

Legislation	Provisions
Labor Protection Act	§ 8 – employers' general duty of care
Labor Protection Act	§ 25 – avoidance and reduction of load
Labor Protection Act	§ 28 – harassment
Law on equality between women and men	Section 7 – discrimination
Penal Code	Section 24 §1a- harassing communication
Penal Code	Section 27 § 3a – violation of personal rights
Penal Code	§ 9 – defamation
Occupational Health Care Act ⁵⁷	§ 1 The purpose of the law.

Table 14. Finnish regulation of workplace cyberbullying⁵⁸

⁵⁵ Law on equality between women and men.

⁵⁶ Criminal Code Section 27 § 3a.

⁵⁷ Occupational Health Care Act (Työterveyslaki (21.12.2001/1383) § 1.

⁵⁸ Edited by the author.

2.3. Cyberbullying in schools

In Finland, since the beginning of the 1990s, public opinion has paid a lot of attention to school bullying. Since the last decade, this focus has also extended to electronic or internet bullying. In Finnish, there are separate expressions for internet bullying (*nettikiusaaminen*) and harassment via mobile phones (*kännykkäkiusaaminen*). The most frequently mentioned forms of cyberbullying in public debates include sending abusive or threatening messages on mobile phones or e-mails, and posting embarrassing or humiliating photos or videos on websites.⁵⁹ In light of the significant media attention and public interest, more research is being conducted on these new forms of bullying.⁶⁰ Some NGOs have conducted surveys on cyberbullying using online questionnaires.

Finnish schools are expected to prevent and deal with bullying among children. The Finnish Basic Education Act⁶¹ (since 1999) states that every student has the right to a safe school environment. Education providers have a responsibility to ensure that students do not experience violence or bullying at school. The legislation affects all levels of education. It was further amended in 2003, stating that the instructor prepares a plan for the protection of students against violence, intimidation and harassment in connection with the development of the curriculum, implements the plan, and supervises its compliance and implementation.

A Finnish study among 12-17-year-olds tried to get answers about online bullying in and outside of schools.⁶² Half of the young people who responded to the survey (50%) said that they had been exposed to some kind of internet bullying at least once. The vast majority of young people (more than 80%) have seen some form of harassment against other people on the Internet. The majority of young people (84%) consider it important that someone protects the bullied.⁶³ Bullying and harassment in one way or another is a daily part of using the Internet and it is difficult to avoid it. The most common form of online harassment was malicious comments and mockery, which 39% of respondents had encountered at least once. 21% of young people reported bullying, in which they spread offensive pictures, videos or rumors about the young person. Some of the bullying experienced by young people was related to the use of their own name for

⁵⁹ Li-Cross-Smith, 2012, p. 57.

⁶⁰ Markus Aarno-Ilmari Kaakinen-Matti Johannes Näsi, Youth Criminal Behavior and Victim Experiences 2020. Institute of Criminology and Legal Policy.

⁶¹ Education Basic Law (21.8.1998/628, Perusopetuslaki) [Online]. Available: <https://www.finlex.fi/fi/laki/ajantasa/1998/19980628>

⁶² Raja, 2021.

⁶³ Raja, 2021, p. 5.

the purpose of bullying or a mocking or fake profile created in the name of the young person. Exclusion or isolation is a form of bullying that affects around one in five young people in digital environments. Exclusion can be, for example, being excluded from social media groups, or being excluded from shared video calls by a class or group of friends. Young people are also worried about the loneliness of young people ‘living’ on the Internet, who are already alone even in their school community.⁶⁴

The young people participating in the survey also reported on other forms of harassment:

- (a) harassing phishers and fraudsters;
- (b) harassment in various online gaming communities;
- (c) harassment by unknown teasers.

The question arises as to what young people can do when they are bullied, how they can reduce the harm done to them. The respondents in the survey gave answers to this as well. Young people can deal with cyberbullying situations in several ways. In a situation where a young person was being bullied themselves, the most common course of action was to block the bully. This was the case for 42% of young people who were bullied on the Internet. The second most common course of action was asking bullies to stop bullying (31%) or telling a friend (31%). About a fifth of bullied youth told a trusted adult, such as a parent or teacher. Similarly, one fifth of the young people filed a complaint and 19% did nothing.⁶⁵

As for gender differences, according to a study in Finland, girls used the tool of cyberbullying significantly more often than Finnish boys. Finnish girls in particular sent nasty text messages, e-mails and posted humiliating pictures on the Internet.

The fact that children are particularly vulnerable to cyberbullying is very difficult to prevent, and this is highlighted by the KU vs. Finland case, when an ad was placed in the name of a 12-year-old child on a dating site without his knowledge. The ad included the applicant’s age, phone number and physical characteristics. The case started at the request of the child’s parents, who asked the Finnish court to oblige the service provider to reveal the identity of the person who posted the ad online. In this case, the ECtHR found Finland to have violated Article 8 of the European Convention on Human Rights, as Finnish law at the time did not oblige internet service providers to disclose the identity of the

⁶⁴ Raja, 2021, p. 6.

⁶⁵ Raja, 2021, p. 9.

perpetrators of crimes such as child sexual abuse. In connection with the case, the ECHR noted that where the child's physical and moral well-being is endangered, such an obligation is even more important.⁶⁶

2.4. Summary

Cyberbullying has now become an everyday phenomenon in Finland as well. In the last decade – as in our country – the continuous expansion of the Internet has become an excellent field for the almost unlimited spread of online harassment and intimidation. In response to this, in Finland, preventive or restorative programs are constantly being developed in educational institutions, but this phenomenon unfortunately regularly appears in and outside of the workplace in addition to young people, so the adult population is also affected. Many forms of cyberbullying are known, so the legal environment in Finland is diverse. The Criminal Code, the Labor Protection Act and the Act on the Equality of Women and Men also contain provisions. Finland is one of the 14 EU member states that has a specific definition of cyberbullying, and the Finnish criminal code also contains provisions that can be applied in the case of cyberbullying. Cyberbullying can include, for example, insulting the victim on a discussion forum or sending mean, unfounded e-mails to the victim.

3. Regulation and practice related to prevention

3.1. Prevention in educational institutions

3.1.1. Presentation of the KiVa program

The KiVa program was developed by internationally recognized researchers of school abuse, Prof. Christina Salmivalli and Elisa Poskiparta (University of Turku), building on their decades of research. Their work was funded by the Finnish Ministry of Education and Culture because public education institutions in Finland have been required by law to act against abuse since 2001, and for this they needed an effective but easy to implement and sustainable program.

One of the program's innovations is that it is both a prevention and intervention program, which means that prevention covers all students, while

66 Dalla Pozza-Di Pietro-Morel-Psaila, 2016, p. 39.

intervention only applies to students involved in abuse.⁶⁷ KiVa is a comprehensive, school-wide program in which members of the KiVa team play a prominent role. They are selected from among the school's teachers and support professionals (developmental pedagogue, school psychologist, social worker), their number is 3-4 – depending on the size and involvement of the school. Their tasks are as follows:

- (a) individual case management;
- (b) ensuring the continuation of the program;
- (c) holding classroom sessions;
- (d) contact with stakeholders;
- (e) participation in parent meetings;
- (f) participation in events promoting the program⁶⁸.

KiVa targets the primary school age group and consists of three parts (Unit1-2-3). The backbone of the program is the so-called Unit2 conveys the most knowledge about abuse (including its hidden forms) to 10-year-old children entering upper school and provides an opportunity to practice behavioral strategies to avoid becoming a target and protect the victim. Unit3 is a kind of reminder, based more on contemporary influence, and indirectly strengthens the maintenance of the anti-abuse norm. In the case of all three units, the date of implementation is a phase change in school life: a new community is created or the group gets a new leader. This increases the effectiveness of the program because it is easy to influence the formation of norms at the beginning of the group formation, and positive peer and teacher-student relationships can also develop.⁶⁹ KiVa is a scientifically based program. Current psychological theories emphasize the role of bystanders in explaining the development and persistence of school abuse. With the help of the affirming reaction of the students observing the abuse (recognition, approval, fear), the abuser obtains the status and power he desires. A student with an abusive character is in almost every class, and there are potential victims everywhere, that is, students who are characterized by several risk factors for becoming a victim.⁷⁰

The key to prevention is therefore the establishment of a group norm against abuse and changing the behavior of bystanders. Therefore, KiVa does not consider the abuser, nor the victim, the primary target of the intervention, but the entire school community. The key to mobilizing bystanders is, on the one

67 Jármi-Péter-Szarka- Fehérpataky, 2012, p. 5.

68 Jármi-Péter-Szarka- Fehérpataky, 2012, p. 5.

69 Jármi-Péter-Szarka- Fehérpataky, 2012, p. 6.

70 Jármi-Péter-Szarka- Fehérpataky, 2012, p. 6.

hand, empathy with the victim (so that, recognizing the victim's suffering, they are motivated to protect him), and on the other hand, knowledge of safe strategies with which they can support the victim. KiVa's goals for observers are as follows:

- (a) increasing empathy;
- (b) strengthening the sense of effectiveness in the field of action against abuse;
- (c) supporting efforts to apply learned behaviors⁷¹.

The program developed by Finland has already been successfully applied by several countries and with its help they were able to substantially reduce the number of cases.

It is important to mention that the introduction of peer mediation, which is one of the defining elements of restorative justice, can be an effective preventive tool. In the event that abuse does occur, the damage can be reduced, and thus the chance of future occurrences can also be mitigated. Research shows that the method of mediation is an extremely effective tool for dealing with conflicts, because the solution is sought together and everyone's opinion is properly expressed.⁷²

3.1.2. Presentation of the VERSO program

In addition to the KiVa program, the VERSO program operates in Finland, which focuses on mediation. Mediation activities in the field of education have been developed and carried out in the VERSO program since 2000. Since 2006, the program has been operating within the framework of the Finnish Mediation Forum, which was founded in 2003.⁷³ VERSO is a non-profit program funded by the Financial Center for Social Welfare and Health Organizations (STEA).

The program offers mediation training in early childhood education, primary and secondary education, enabling both teachers and pupils/students to act as mediators in controversial or conflict situations. The VERSO program offers its participants concrete methods for organizing restorative meetings and offers an alternative solution for resolving conflicts between children and between children and school staff. During restorative mediation, children learn

⁷¹ Jármi-Péter-Szarka- Fehérpataky, 2012, p. 6.

⁷² Lappalainen-Perälä, 2015, pp. 5–6. He.

⁷³ Gellin, 2018, p. 254.

emotional and communication skills, as well as responsibility for their own actions.⁷⁴

Peer or adult mediators trained by the VERSO program help parties in conflict to resolve their disputes. In restorative mediation, the child is not stigmatized, but respected and listened to as an expert in his own conflict and its resolution. The parties are encouraged to tell their side of the story, describe their feelings and needs, and think about possible solutions. After finding solutions, the parties conclude an agreement, which is monitored later.

The goal of the VERSO program is to reduce and mitigate school conflicts by improving communication. Mediation activities in schools do not eliminate other forms of intervention, but offer an additional tool for early and child-friendly handling of different types of conflicts. The goal of the VERSO program is to initiate and strengthen peer mediation and voluntary mediation activities led by children and adults in educational institutions. In addition, VERSO aims to support the development of a restorative culture in these institutions through local mentoring activities.

The objectives of the program can be divided into the following groups:

- (a) Prevention of bullying in schools and early childhood education institutions, as well as early response to bullying situations with community and participatory processes. These processes respect and prioritize the rights of the child in accordance with the early childhood education curriculum, the national core curriculum, the UN Declaration on the Rights of the Child and the Council of Europe guidelines on child-friendly justice;
- (b) Support for peer mediation, voluntary restorative mediation activities for pupils/students and staff, and mentoring activities in schools, ensuring a safe and calm work environment to reduce bullying and harassment;
- (c) Strengthening the mediation activity;
- (d) Strengthening regional cooperation and networking among actors trained by VERSO (staff, children, pupils/students, parents/guardians) through mentoring activities.⁷⁵

In 2019, 89 schools provided information on how many mediated cases there were in the institutions. During the year, the number of cases mediated by peer mediators in these schools was 2,033. Cases referred to mediation were predominantly verbal (49%) and physical abuse (37%).⁷⁶

⁷⁴ Olkkonen, 2020, p. 1.

⁷⁵ Olkkonen, 2020, p. 2.

⁷⁶ Olkkonen, 2020, p. 7.

Case type	Incidence rate
Verbal insult	49%
Mental abuse	37%
Attack on personal property	6%
Exclusion	4%
Other	4%

Table 15. Background of cases resolved by mediation in the Finnish school system⁷⁷

A very important argument in favor of the VERSO program is that peer-to-peer mediation is very effective, as it produced great results in every year examined (2017-2019). In 2019, an agreement was reached in 95.9% of the mediated cases, and 91.5% of the agreements were respected.⁷⁸

One of the proofs of the success of the mediation program is that the participants were asked to indicate the aspects that are important in relation to restorative mediation. The following three aspects were mentioned most often:

- (a) Everyone has the opportunity to tell their own story (75%);
- (b) Discussing feelings and needs (selected by 54%);
- (c) There is no penalty in mediation, but they look for a solution (54%).⁷⁹

3.2. Recommendations of the working group for more effective action against hate speech and cyberbullying

From the point of view of prevention, it is important to call into existence and consider the recommendations of such working groups as the Working Group for More Effective Action Against Hate Speech and Internet Harassment. The working group formulated recommendations for the government and its institutions that can help to take more effective action against hate speech and online harassment:

- (a) The Government should prepare an action plan against hate speech;
- (b) Creating a center of excellence, making more research, more information available and strengthening knowledge-based management;
- (c) Overview of legislation;
- (d) Expanding the liability of online platforms;
- (e) Giving the media more opportunities to fight hate speech;
- (f) More support for victims of hate speech;

⁷⁷ Edited by the author.

⁷⁸ Olkkonen, 2020, p. 7.

⁷⁹ Olkkonen, 2020, p. 10.

- (g) Holding the employer accountable if an employee is subjected to hate speech or hate campaigning;
- (h) Provide more information and training on hate speech and freedom of speech and its limits;
- (i) Improving media literacy;
- (j) More effective measures to combat religious and religion-based hate speech;
- (k) Preparing teachers to combat hate speech and cyberbullying.⁸⁰

The Finnish Ministry of Justice has launched a project in this area. The project's goal is to strengthen the fight against hate crimes and online hate speech in Finland. It focuses on improving the legislative framework and enhancing cooperation between authorities, with particular emphasis on better identifying and investigating hate-motivated crimes. Additionally, the project aims to raise public awareness and support the legal protection of victims⁸¹.

Another project's goal is to improve the regulation of online platforms in Finland to ensure the safety of digital services and protect users' rights. The project examines the implementation of the EU-level Digital Services Act and the alignment of national regulations. It also aims to involve the public and market players to ensure that regulatory frameworks address the challenges of the modern digital environment.⁸²

3.3. Summary

When we talk about the prevention of cyberbullying or cybercrime, it can be stated that Finland provides exceptionally large resources for prevention, even in comparison with the EU. Several successful programs (VERSO, KiVa) have already been created, which have been successfully adapted in many countries around the world and were able to prove with subsequent research that they really cause a significant drop in cases if these programs are carried out throughout. It is characteristic of Finland that the effective prevention of cyberbullying is treated as a priority area by society, the media and politicians. The highly praised KiVa School program is reported to be ineffective based on feedback

⁸⁰ Words Are Actions More Efficient Measures against Hate Speech and Cyberbullying, 2019, p. 15.

⁸¹ Against hate -projekti (OM005:00/2018) Available: <https://oikeusministerio.fi/en/project?tunnus=OM043:00/2018>

⁸² Fact against hate (OM043:00/2019) Available: <https://oikeusministerio.fi/en/project?tunnus=OM043:00/2019>

from bullied students, and it is sometimes used in harmful ways, according to bullying prevention expert Tina Holmberg-Kalenius. She states that the issue lies not within the program itself but in the improper application by some schools. The Kiva program, aimed at combating school bullying, can even exacerbate bullying in certain contexts.⁸³

4. Responsibility of service providers and institutions

4.1. Responsibility of service providers

While social media platforms offer a useful space for obtaining information, sharing, and commenting on opinions, people can still be silenced by the fear of hate speech and insults on the internet. As a result, expanded freedom of expression may actually narrow the range of opinions and information shared⁸⁴. In the Finnish legal environment – in addition to EU regulations – several laws specify the responsibility of service providers.

Legislation	The relevant provisions
The Act on Electronic Communications Services	Information security, content provision
Criminal Code	38:4 if the perpetrator misuses their position in a telecommunications company.
Data Protection Act	Protection of personal data

Table 16. Finnish legislation governing the liability of service providers⁸⁵

The Act on Electronic Communications Services is a key element of the regulation of digital communication and content provision in Finland.⁸⁶

The law contains provisions on issues such as information security and the security of confidential communication channels. The law also applies to

⁸³ The acclaimed Kiva School program is reportedly used in harmful ways, as it “leaves considerable trauma for the bullied.” <https://yle.fi/aihe/artikkeli/2019/01/09/ylistettya-kiva-koulu-ohjelmaa-kaytetaan-jopa-vahingollisella-tavalla-jattaa>

⁸⁴ Korpisaari (ex. Tiilikka), Päivi (2022) From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments?: An analysis of the practice of the ECtHR and some reflections on the Digital Services Act.

⁸⁵ Edited by the author.

⁸⁶ The Act on Electronic Communications Services (917/2014, Laki elektronien viestinänn palveluista). [Online]. Available: <https://www.finlex.fi/fi/laki/ajantasa/2014/20140917>

telecommunications providers, communications providers, corporate or association subscribers and domain name registrars. The obligations of the relevant service providers regarding information security and the security of confidential communication are defined separately by law.

The telecommunications service provider may be obliged to remove illegal content in the event that a service provider related to the information society, such as a content download service, is not available. This can prevent, among other things, the commission of crimes against children. According to the previous regulations, it was practically impossible to remove illegal content if the service provider was unknown or located abroad.

The law implements the measures of the EU common toolkit for the security of 5G networks in order to protect key parts of the communication network. In the communication network, it is forbidden to use a communication network device, the use of which could endanger national security. The regulation also applies to ad hoc networks connected to certain public communication networks.

The Finnish Criminal Code does not include the term cybercrime, instead cybercrimes are typically classified Data and communications offenses crimes (Chapter 38). In addition, Criminal Code its other chapters also contain provisions for other crimes related to cybercrime (business secret violation and abuse). Recent discussions on 'cybercrime' focus on whether the phenomenon is genuinely new or not. Some authors argue that cybercrime is not significantly different from 'terrestrial crime' and can be explained using traditional criminological theories. One such approach is the routine activity theory developed by Marcus Felson.⁸⁷

An outstanding achievement in regulating the responsibility of service providers is the creation of a new Network Security Advisory Board (the mandate of the Advisory Board begins on February 15, 2021 and lasts until June 30, 2022)⁸⁸ to oversee the security of communication networks. Key authorities representing various sectors of government and the telecommunications industry are represented in the Advisory Board. The Advisory Board deals extensively with issues related to the security of communication networks and, where appropriate,

87 Majid, Y. (2005). The Novelty of 'Cybercrime'An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* 2(4):407-427. Available: https://www.researchgate.net/publication/238433587_The_Novelty_of_'Cybercrime'An_Assessment_in_Light_of_Routine_Activity_Theory/link/00b495327859daf12a000000/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

88 Network Security Advisory Board (Verkkoturvallisuuden neuvottelukunta), <https://valtioneuvosto.fi/hanke?tunnus=LVM026:00/2021>

makes recommendations to improve network security. The task of the Advisory Board is to assess and develop the security of domestic communication networks, as well as to support official decision-making. The Advisory Board may also deal with other issues related to cyber security determined by the government.

The GDPR and the Finnish data protection law also plays a role in promoting cyber security, which basically regulates the responsibilities of data controllers and data processors and the role of the data protection ombudsman. The data manager and the data processor take appropriate and specific measures to protect the rights of the data subject, which can help prevent some online crimes and is primarily of data protection importance. Such measures include:

- a) measures that enable subsequent verification of the identity of the person recording, changing or transmitting personal data;
- b) measures to improve the competence of personnel processing personal data;
- c) appointment of a data protection officer;
- d) internal measures of the data controller and data processor to prevent access to personal data;
- e) encryption of personal data;
- f) measures that ensure the ongoing confidentiality and integrity of data processing systems and services related to the processing of personal data;
- g) a procedure for regularly testing, evaluating and evaluating the effectiveness of technical and organizational measures ensuring the security of data processing.⁸⁹

4.2. Employers

Workplaces also play a significant role in preventing online bullying. The Occupational Safety and Health Act prohibits inappropriate treatment and workplace harassment. It imposes obligations on employers and employees. According to the law, if harassment or other inappropriate treatment of an employee occurs at the workplace and causes danger or risk to the employee's health, the employer is obliged to take measures to remedy this.

According to the law, the employer is obliged to take care of the safety and health of his employees during work by taking the necessary measures. To this end, the employer must take into account the work-related circumstances, other

⁸⁹ Data Protection Act (1050/2018) Section 6.

aspects of the work environment, as well as the personal abilities of the employees. Unusual and unforeseeable circumstances beyond the employer's control, as well as extraordinary events whose consequences cannot be avoided despite due diligence, are taken into account as factors limiting the scope of the duty of care.⁹⁰

Employers are obliged to plan the measures necessary to improve working conditions, as well as to decide on the extent and practical implementation of the measures. Accordingly, the following principles should be observed to the greatest extent possible:

- a) prevention of hazards and risk factors;
- b) eliminating hazards and risk factors or, if this is not possible, choosing a less dangerous or harmful alternative;
- c) adoption of general security measures;
- d) taking technological development and other available tools into account.

Employers must constantly monitor the work environment, the state of the workplace community and work safety. Employers must also monitor the impact of the measures introduced in practice on workplace safety and health protection. Employers ensure that safety and health measures are properly taken into account in the operation of each part of their organizations.

An important provision of the law is that employers must also develop an occupational health and safety policy, the purpose of which is to promote safety and health protection, as well as to develop the necessary measures to preserve the ability of employees to work. The regulations must include the need to improve working conditions and the impact of work environment factors. During workplace development and planning, the objectives of promoting safety and health and preserving working capacity arising from the regulations must be taken into account, and they must be discussed together with the employees or their representatives.

4.3. Educational institutions

4.3.1. Anti-bullying laws in Finnish schools

In order to make the school environment safer, the Finnish Education Act (*Perusopetuslaki*) changed at the beginning of the last decade and underwent a major amendment, as a result of which the educational service provider was required

⁹⁰ Occupational Health and Safety Act, Chapter 2, Section 8.

to prepare a plan regarding the prevention of bullying and the protection of students against violence and bullying. in order to implement this plan, as well as supervise its implementation. This provision means that the legislation prescribed the preparation and implementation of the plan as an institutional obligation of the schools⁹¹. The plan for the prevention and treatment of school bullying must include the following mandatory content elements:

- a) Intervention in cases of harassment and violence;
- b) Treatment at community, group and individual levels;
- c) Individual support for the victim;
- d) Cooperation with parents;
- e) Cooperation with necessary officials;
- f) Presentation and communication of the plan to the stakeholders.

Educators must implement the plan and monitor its completion and compliance, as this is essential to ensuring an ongoing safe learning environment.

Well-functioning preventive and restorative programs are already available to educational institutions. The KiVa program, already presented in detail above, was developed at the University of Turku and was financed by the Finnish Ministry of Education and Culture. It has already been used in 30% of Finnish educational institutions and has achieved surprisingly good results.

4.4. Summary

Based on the Finnish regulations, although hate speech does not have a specific legal status, it can already be seen during the analysis of the Finnish constitution that it contains specific measures that already constitutionally try to prevent hate speech. These provisions are provisions on the prohibition of discrimination and the protection of human dignity. Hate speech is not specifically regulated in the Finnish Criminal Code either, but it is linked to several crimes depending on whether the motives characteristic of hate crimes appear in the committed crime. Statistical data shows that hate speech is a persistent issue in the lives of Finnish citizens, and limiting it online is challenging. Many preventive campaigns support efforts to address this issue, and research in this area continues. Recent studies have highlighted that hate speech can significantly affect social participation and opinion formation among individuals.

Cyberbullying is now commonplace in Finland as well. In the last decade the continuous expansion of the Internet has become an excellent field for the

⁹¹ Farmers, 2021, p. 22.

almost unlimited spread of online harassment and intimidation. In response to this, preventive or restorative programs are available in educational institutions in Finland, but this phenomenon unfortunately regularly appears in and outside of the workplace in addition to young people. Finland is one of the 14 EU member states that has a specific definition of cyberbullying, and the Finnish criminal code also contains provisions that can be applied in the case of cyberbullying. When we talk about the prevention of cyberbullying or cybercrime, it can be stated that Finland provides an outstanding amount of resources for prevention, even in comparison with the EU. Several successful programs (VERSO, KiVa) have already been created, which have been successfully adapted in many countries of the world and were able to prove with subsequent research that they really cause a significant drop in the number of cases if these programs are carried out. Effective protection requires adequate data protection, the development of appropriate workplace strategies, the development of harassment prevention policies, and the protection of younger generations is also very important, which is the fundamental obligation of educational institutions laid down in law. In this area, there are significant differences compared to the Hungarian system, as the Finns devote a significant amount of resources to effective prevention and treatment programs, which have been successfully exported to many other countries, so the KiVa program is well known in our country as well. The study published by the University of Helsinki examines the legal regulation and occurrence of hate speech and hate crimes in Finland, with a focus on cases registered by the police. The research highlights that the number of incidents motivated by ethnic and religious hatred is on the rise.⁹²

92 Korpisaari (ex. Tiilikka), Päivi (2022) From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments? : An analysis of the practice of the ECtHR and some reflections on the Digital Services Act.

Bibliography

- Dalla Pozza, V., Di Pietro, A., Morel, S., Psaila, E. (2016) *Cyberbullying Among Young People*. Directorate General for Internal Policies. Policy Department C: Citizen's Rights and Constitutional Affairs Civil Liberties, Justice and Home Affairs. Study for the LIBE Committee
- Gazdek, H. (2021) *The anti-cyberbullying programs in Finnish lower secondary schools: Teacher perspectives*. Faculty of Education and Psychology, University of Jyväskylä, Master's Thesis in Education Spring Term
- Gellin, M. (2018) *Mediation in Finnish Schools: From Conflicts to Restoration*. Nordic Mediation Research, Finnish Forum for Mediation, Helsinki.
- Hallamaa, J. (2019) 'Päivi Räsänen vihapuheperössi krököllis-polittisena performansina (The process of hate speech from a religious and political perspective)', *Kanava*, 47(8)
- Hoel, H., Vartia, M. (2018) *Bullying and sexual harassment at the workplace, in public spaces and in political life in the EU*. Policy Department for Citizen's Rights and Constitutional Affairs.
- Jaghoory, H., Björkqvist, K., Österman, K. (2015) 'Cyberbullying among Adolescents: A Comparison between Iran and Finland', *Journal of Child and Adolescent Behavior*, 3(6)
- Järmi, É, Péter-Szarka, Sz, Fehérpataky, B. (2012) *The possibility of domestic adaptation of the KiVa program*. Educational Research and Development Institute
- Knuutila, A., Kosonen, H., Saresma, T., Haara, P., Pöyhtäri, R. (2019) 'Viha vallassa: Vihapuheen säätössällisein säättekoon (Anger in power: the impact of hate speech on decision-making)', *Valtioneuvosto survey – ja tutkimusinnin jaluiksusarja (Research activities publication series)*, 2019/57. [Online]. Available at https://julkaisut.valtioneuvosto.fi/bitstream/handle/10024/161812/57_19_Viha%20vallassa_Vihapuheen%20väktein%20_Netti%20.pdf
- Lappalainen, E., Perälä, P. (2015) *Vertaissovittelu alakouloisten sovittelioijden sikkeit (Contemporary media for primary school students)*. Kasvatustieteen gradu -tutkielma Syyslukukausi
- Li, Q., Cross, D., K. Smith, P. (2012) *Cyberbullying in the Global Playground: Research from International Perspectives*. Hoboken: Blackwell Publishing Ltd.
- Mäkinen, K. (2019) 'Sanat ovat tekoja: Vihapuheen ja nettikiusaamisen vastaisten toimien tehostaminen (Words are actions: stepping up action against hate speech and cyberbullying)', *Sisäministeriön jülüksujaja (Publications of the Ministry of the Interior)*, 2019/23.
- McCully, J. (2019) *Legal Responses to Online Harassment and Abuse of Journalists: Perspectives from Finland, France and Ireland*. OSCE – Office of the Representative on Freedom of the Media & International Press Institute

- Olkkonen, K. (2020) *VERSO Program Annual Report*. The Finnish Forum for Mediation, Helsinki.
- Pöyhtäri, R., Haara, P., Raittila, P. (2013) *Vihapuhe Sananvapautta Kaventamassa (Hate Speech as Restriction of Expression)*. Tampere University Press
- Raja, R. (2021) *Nuoret ja nettikiusaminen (Young people and cyberbullying)*. Mannerheimin Lastenseurgelliitto [Online]. Available at <https://cdn.mll.fi/prod/2021/04/21124054/nuoret-ja-nettikiusaaminen-kyselyraportti-mll-2021.pdf>
- Markus, A., Ilmari, K., Matti J. N.(2020), Youth Criminal Behavior and Victim Experiences 2020. Institute of Criminology and Legal Policy
- Perspectives on Platform Regulation: Concepts and Models of Social Media Governance Across the Globe (2021) – <https://helda.helsinki.fi/server/api/core/bitstreams/ce499b09-fea8-4e25-a846-3e222f937552/content> pp. 473–485.
- Poliisin tietoon tullut viharikollisuus Suomessa 2018 (Hate Crimes Reported to the Police in Finland 2018) – Available: <https://www.theseus.fi/handle/10024/261556>
- Korpisaari (ex. Tiilikka), Päivi (2022) From Delfi to Sanchez – when can an online communication platform be responsible for third-party comments?: An analysis of the practice of the ECtHR and some reflections on the Digital Services Act
- Majid, Y. (2005). The Novelty of ‘Cybercrime’An Assessment in Light of Routine Activity Theory. *European Journal of Criminology* 2(4):407-427. Available: https://www.researchgate.net/publication/238433587_The_Novelty_of_‘Cybercrime’An_Assessment_in_Light_of_Routine_Activity_Theory/link/00b495327859daf12a000000/download?_tp=eyJjb250ZXh0Ijp7ImZpcnN0UGFnZSI6InB1YmxpY2F0aW9uIiwicGFnZSI6InB1YmxpY2F0aW9uIn19

XV. HATE SPEECH, CYBERBULLYING AND THE DIFFICULTY OF DETECTING CRIME IN ONLINE SPACE – THE EXAMPLE OF THE UNITED KINGDOM

ÁGNES JUHÁSZ

1. Regulation of hate speech

In the United Kingdom, freedom of expression is regulated by the Human Rights Act 1998 (hereinafter referred as to HRA)¹, by incorporating the rights set out in the European Convention on Human Rights (after this referred to as ECHR). According to Article 12(1) HCR, everyone has the right to freedom of expression. This right includes the freedom to hold opinions on the one hand, and to receive and impart information and ideas. On the other hand. Article 12(2) states that exercising of this freedom may be subject to such formalities, conditions, restrictions, or penalties. For instance, freedom of expression can be restricted to protect the reputation or rights of others.

The use of hateful expressions, as in other countries, is negatively perceived in the UK. Acts motivated by hate cover a wide range of acts including criminal offences (hate crimes) and non-criminal hate incidents. The term ‘hate speech’ is a broader expression that covers both criminal and non-criminal acts.

The existing set of rules on hate speech is the result of several centuries of evolution. It overarches the branches of law combining the provisions of constitutional law, criminal law, and civil law. In this development process, the last five decades have been particularly important, as the elaboration of the

¹ Available at <https://www.legislation.gov.uk/ukpga/1998/42/contents>

anti-discrimination rules and the development of the international regulation of human rights took place in this period.

Hate crimes are regulated by the rules on the protection of the public order. However, the applicability of the related provisions depends on the place where the given act was committed. Whereas similar rules are applicable to hate crimes in England, Scotland, and Wales, Northern Ireland adopted its regulation on hate crimes, even if these rules fully comply with the regulations of the other three parts of the UK.

In the following, provisions related to hate crimes are reviewed according to the parts of the UK.

1.1. England, Scotland, and Wales

Provisions aimed at treating the use of expressions inciting racial hatred appeared first time in 1965, during the fight against racial discrimination. The adoption of these rules was a sort of legislative response to the immigration waves of the 1950s and 1960s, and the incidents motivated by racial discrimination that became more and more common at that time.

Race Relations Act 1965 (referred to as RRA) was adopted to regulate different acts motivated by racial discrimination. Article 6(1) RRA provided on the incitement to racial hatred qualifying it as unlawful. Incitement to racial hatred could be committed by the publishing or distributing or written matter having a threatening, abusive, or insulting nature. Moreover, the offence of incitement to racial hatred is committed if a person uses in any public place or at any public meeting words which are threatening, abusive, or insulting. In both cases, it is required that the person committing the offence acts with intent to stir up hatred against any section of the public in Great Britain distinguished by colour, race, or ethnic or national origin, or the act is likely to stir up hatred against any section distinguished by the mentioned characteristics.

From the 1970s, provisions on racial hatred were highly debated which later resulted in the amendment of these rules.

Rules on racial hatred are contained by the Part III of the Public Order Act 1986 (hereinafter referred to as POA).² In 2023, a new Public Order Act was passed, amending the provisions of the POA 1986 in several places. However, the provisions on racial hatred remain unchanged.

At the beginning of Part III, the meaning of racial hatred is clarified. According to Article 17, racial hatred, in the application of Part III POA, means hatred

² Available at <https://www.legislation.gov.uk/ukpga/1986/64/contents>

against a group of persons defined by reference to colour, race, nationality (including citizenship), or ethnic or national origins. However, the interpretation of this article arises further questions regarding the term ‘race’.^{3,4} After this clarification of racial hatred, Part III POA provides rules on different criminal offences by which the person committing the act intends to stir up racial hatred or racial hatred is likely to be stirred up thereby.

According to Article 18(1) POA, the use of threatening, abusive, or insulting words or behaviour, or displaying any written material which is threatening, abusive, or insulting, is an offence, if the act intends to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. Similarly, the publishing or distributing of written material having the same features, i.e. it is threatening, abusive, or insulting, is also an offence provided that the person committing the act intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. (Article 19(1) POA)

The legislator also takes into consideration if threatening, abusive, or insulting words are used within the framework of a public performance. According to Article 20(1) POA, any person who presents or directs a public performance of play commits an offence, if the performance involves the use of threatening, abusive, or insulting words or behaviour and the person intends thereby to stir up racial hatred, or, having regard to all circumstances, and, in particular, taking the performance as a whole, racial hatred is likely to be stirred up hatred. In the lack of such intention, the person who presents or directs the performance can be revealed from the responsibility, if the fulfilment of either of the circumstances declared in points (a)-(c) of Article 20(2) can be proven by this person. For defence, the person presenting or directing the performance shall prove that he did not know and had no reason to suspect that (a) the performance would involve the use of the offending words or behaviour, or (b) the offending words or behaviour were threatening, abusive or insulting, or (c) the circumstances in which the performance would be given would be such that racial hatred would be likely to be stirred up.

According to Article 21(1) POA, distributing, showing, or playing any recording of visual images or sounds which are threatening, insulting or abusive, is a

3 Certain ethno-religious groups such as Jews and Sikhs have been recognised as racial groups in law in addition to being religious groups, while Roma, Romani Gypsies and Irish Travellers (‘GRT’) are also recognised racial groups based on their ethnic origins. Cf. *Mandla v Dowell Lee* [1983] 2 AC 548, [1983] 2 WLR 620; *Commission for Racial Equality v Dutton* [1989] QB 783, [1989] 2 WLR 17; *O’Leary v Punch Retail* (29 Aug 2000).

4 Neller, 2023, p. 285.

criminal offence if this act intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby. In those cases when a given broadcasting or programme contains threatening, abusive, or insulting visual images or sounds, not only the person who provides the programme service, but those by whom the programme is produced or directed or by whom the offending words or behaviour are used, shall be guilty of committing criminal offence.) Article 22(2) POA) Nevertheless, the perpetration of the above-mentioned criminal offence can only be assessed if the person intends thereby to stir up racial hatred, or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby.

Part III POA devotes a separate section for the racially inflammatory materials. The mere possession of written material or a recording of visual images or sounds which is threatening, abusive or insulting, is a criminal offence, if the written material is being displayed, published, distributed, the recording is being distributed, shown, played, or both kind of materials are included in a cable programme service, whether by himself or another. (Article 23(1) POA) Similarly to other acts, these acts can only be assessed as criminal offence if the act of the person committing is purposeful. By committing the act, the person intended to stir up hatred or, having regard to all the circumstances, racial hatred is likely to be stirred up thereby.

It shall be noted that guilt of a legal entity (body corporate) also can be established in the case of committing the above-mentioned acts. In those cases when the act is committed with the consent or connivance of a director, manager, secretary or other similar officer of the body or a person purporting to act in any such capacity, both the person committing the act and the body corporate are guilty of the offence and liable to be proceeded against and punished accordingly. (Article 28(1) POA)

In October 2007, after countless failed attempts, incitement to religious hatred was criminalised and POA was supplemented with a new part (Part 3A).⁵ From March 2010, following a recent amendment of the POA and the heading of Part 3A as well, Part 3A covers other offences based on hatred against

⁵ Part 3A was inserted by the Racial and Religious Hatred Act 2006. For examples from the related literature, see Cumper, Peter: Outlawing incitement to religious hatred – a British perspective, In: *Religion and Human Rights*, Vol. 1 (2006) No. 3, pp. 249–268; Hare, Ivan: Crosses, Crescents and Sacred Cows. Criminalising Incitement to Religious Hatred, In: *Public Law*, 3/2006, pp. 521–538; Thompson, Simon: Freedom of expression and hatred of religion, In: *Ethnicities*, Vol. 12 (2012), Issue 2, pp. 215–232, McGuire, Kim-Salter, Michael: Legal Responses to Religious Hate Crime: Identifying Critical Issues, In: *Kings Law Journal*, Vol. 25 (2014) Issue 2, pp. 159–184.

persons on grounds of sexual orientation.⁶ These amendments of the POA were important milestones in the regulation of hate crimes since acts motivated by hatred against persons on religious hatred or grounds of sexual orientation were separated from racial hatred. Comparing these two branches of offences, some essential differences can be outlined. In the case of the former, either the conduct of the person or the material possessed by the person shall have a threatening nature, but the abusive or insulting character is not required. Moreover, acts stirring up religious hatred or hatred on the grounds of sexual orientation qualifies as a criminal offence only in those cases when the act of the person is intentional. Acts which are likely to stir up hatred cannot be assessed as a criminal offence.

Nevertheless, regarding the delimitation of racial and religious hatred, it shall be noted that the boundaries between them are sometimes blurred. While some religions are practised worldwide (e.g. Christianity, Islamism), other religions are specifically linked to a particular ethnic group, although their practice is not territorially defined (e.g. Judaism). In Britain, the judicial practice established the category of ‘mono-ethnic’ faith (e.g. Judaism, Sikhism).⁷ However, the distinguishing between ‘race’ and ‘religion’ is not always clear which makes difficult to assess if a certain act motivated by hatred should be deemed under the rules on racial hatred or religious hatred.⁸

The structure of Part 3A practically wholly complies with the Part III of the POA. Introductory provisions intend to make clear the basic expressions. According to Article 29A POA, in the application of Part 3A, the expression ‘religious hatred’ means hatred against a group of persons defined by reference to religious belief or lack of religious belief. The POA, however, does not define what amounts to a religion or a religious belief. In the absence of a specific legal provision, it is for the courts to determine whether a case involves religion or religious belief. It can be said that Article 29A can be applied in the case of widely recognised religions like Christianity, Islam, Hinduism, Judaism, Buddhism, Sikhism, and Rastafarianism, while branches or sects within a religion

6 For the comprehensive discussion of the problem of hatred against persons on grounds of sexual orientation see Goodall, Kay: Challenging hate speech: incitement to hatred on grounds of sexual orientation in England, Wales and Northern Ireland, In: *The International Journal of Human Rights*, Vol. 13 (2009), Issue 2-3, pp. 211–232.

7 Cf. *Mandla v Dowell Lee* [1983] 2 AC 548. The case is reviewed and analysed by Neller. See Neller op. cit. p. 287.

8 About this problem see in details Goodall, Kay: Incitement to Religious Hatred: All Talk and no Substance?, *The Modern Law Review*, Vol. 70, No. 1 (Jan., 2007), pp. 89–113, Neller op. cit. p. 285, Hare op. cit. 534.

can be considered as religious beliefs. The lack of religious belief also can be the ground for religious hatred.

‘Hatred on the grounds of sexual orientation’ means hatred against a group of persons defined by reference to sexual orientation whether towards persons of the same sex, the opposite sex, or both. (Article 29AB POA)

Among the hate crimes covered by Part 3A POA, the legislator first sets out various cases of incitement to hatred based on religious and sexual orientation, which are fully compatible with the situations set out in Part III POA. It is a criminal offence to use threatening words or behaviour, or display any written material that is threatening if the person committing the conduct intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation (Article 29B POA) It is important to note that the in this case, contrary to hate speech based on racial hatred, the offence can only be established if the conduct is purposeful, and the suitability of the conduct to incite hatred does not in itself provide a basis for criminalising the conduct. The act may be committed in a public or private place. However, the act is not a criminal offence if the place where the words or behaviour are used, or the written material is displayed, by a person inside a dwelling and is not heard or seen except by other persons in that or another dwelling.⁹

The publishing or distributing of written material that is threatening is an offence if the person committing the act intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29C(1) POA). Similarly, any person who presents or directs a public performance that involves the use of threatening words or behaviour, is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29D(1) POA) According to the POA, distributing, showing, or playing a recording of visual images or sounds which are threatening is an offence if the person intends to stir up religious hatred or hatred on the grounds of sexual orientation with his act. (Article 29E(1) POA) In those cases when a given programme containing threatening visual images or sounds is included in a programme service, the person providing the programme service, and any person by whom the programme is produced or directed, or by whom offending words or behaviour are used, is guilty of an offence if he intends thereby to stir up religious hatred or hatred on the grounds of sexual orientation. (Article 29F POA)

9 In the application of Part III POA, a ‘dwelling’ means any structure or part of a structure occupied as a person’s home or other living accommodation (whether the occupation is separate or shared with others) but does not include any part not so occupied, and for this purpose ‘structure’ includes a tent, caravan, vehicle, vessel or other temporary or movable structure. (Article 29 POA).

In the case of criminal offences regulated by Part 3A POA, religious groups or grounds of sexual orientation are the target of the hate speech. However, there are other cases when religion is not the characteristic of why the group of persons are attacked, but the source of hate speech. These kinds of religiously motivated expressions are often critical and hostile towards same-sex relationships, therefore, a special dimension of the right to expression, i.e. the right to religious expression and the protection against hate speech (homophobic speech) is in conflict.¹⁰¹¹

After the regulation of the above-mentioned criminal offences which intend to stir up racial hatred, religious hatred, or hatred on the grounds of sexual orientation, Part 3A POA provides rules on the inflammatory materials. According to Article 29G POA, it is a criminal offence if a person possesses written material or recording of visual images or sounds that have a threatening nature, provided that the written material is displayed, published, distributed, or included in a programme service, or the recording is being distributed, shown, played, or included in a programme service, whether by himself or another. Likewise, both the intentional nature of the committing act and the purpose of stirring up hatred are required to deem the act as a criminal offence.

After the taxation of the different criminal offences, Articles 29J and 29JA declare the protection of freedom of expression and highlight separately the freedom of expression on sexual orientation. Article 29J POA, according to the Marriage (Same Sex Couples) Act 2013, states that the discussion or criticism of sexual conduct or practices or the urging of persons to refrain from or modify such conduct or practices shall not be taken of itself to be threatening or intended to stir up hatred. The same is true for marriage: any discussion or criticism of marriage that concerns the sex of the parties to marriage shall not be taken of itself to be threatening or intended to stir up hatred.

In 2021 the Scottish Parliament adopted the Hate Crime and Public Order (Scotland) Act¹² which prescribes the application of provisions other than the rules of POA in Scotland. On the other hand, the Scottish Act will amend or repeal several provisions of Part 3A of the POA.

Although the act maintains the existing legislative protections from crimes aggravated by prejudice towards race, religion, disability, transgender identity,

10 For the related case law, see *Hammond v Department of Public Prosecutions* (2004) EWHC 69

11 See in more detail: Edge, Peter W.: *Oppositional Religious Speech: Understanding Hate Preaching*, In: *Ecclesiastical Law Journal*, Volume 20 (2018) Issue 3, pp. 278-289; Foster, Steve: *Accommodating Intolerant Speech: Religious Free Speech versus Equality, and Diversity*, In: *European Human Rights Law Review*, No. 6/2019, pp. 609-625.

12 Available at <https://www.legislation.gov.uk/asp/2021/14/contents>

and sexual orientation, it introduces new protections against offences aggravated by prejudice towards a person's age. Moreover, it redefines the term 'transgender identity' by removing the term 'intersexuality' and adding the term 'variations in sex characteristics.'

The applicable provisions of the act were highly debated. Some authors expressly argued that the legislation threatens freedom of expression.¹³ Finally, after more than four years, the legislation was implemented on 1st April 2024.

1.2. Northern Ireland

In Northern Ireland, incitement to hatred has been a criminal offence since 1970 when the *Prevention of Incitement to Hatred Act* (hereinafter referred to as PIHA) was adopted. According to Article 1 PIHA a person shall be guilty of an offence if, with intent to stir up hatred against, or arouse fear of, any section of the public in Northern Ireland, he publishes or distributes written or other matter which is threatening, abusive or insulting, or uses in any public place or at any public meeting words which are threatening, abusive or insulting.

This act was replaced by the Public Order (Northern Ireland) Order 1981. The adoption of this act resulted in the insertion of the criminal offence of incitement to hatred into a wider public law regulatory framework. However, its life was quite short, since in 1987, a new Public Order (Northern Ireland) Order¹⁴ (hereinafter referred to as POO) was adopted which is still in force nowadays, even though it has been amended several times.

Part III of POO contains rules on stirring up hatred and, at the same time, on the act arousing fear.¹⁵ The separation of the expressions 'stirring up hatred' and 'arousing fear' is a basic element of the regulation of Northern Ireland. Moreover, the use of the expression 'arousing fear' is an important difference between POO and POA which is applicable in England, Scotland, and Wales since the latter act does not contain this expression at all.

At the beginning of Part III POO, the terms 'fear' and 'hatred' are explained. According to Article 8(1) POO, 'fear' means fear of a group of persons defined by reference to religious belief, sexual orientation, disability, colour, race, nationality (including citizenship), or ethnic or national origins, while 'hatred' means hatred against a group of persons defined by reference to religious belief, sexual orientation, disability] colour, race, nationality (including citizenship) or ethnic

¹³ Bechtold, 2022.

¹⁴ Available at <https://www.legislation.gov.uk/nisi/1987/463/contents>

¹⁵ It is worth noting that POO does not take the expression 'incitement to hatred' from the previous act of 1981.

or national origins. Sexual orientation and disability are a group-forming characteristic from 2004, when POO was amended.¹⁶ After the clarification of the terms 'fear' and 'hatred', POO declares that any discussion or criticism of marriage which concerns the sex of the parties to marriage is not to be taken of itself to be threatening, abusive or insulting, or intended to stir up hatred or arouse fear. (Article 8(2) POO).¹⁷

Article 9(1) POO declares that a person who uses threatening, abusive, or insulting words or behaviour, or displays any written material which is threatening, abusive, or insulting, is guilty of an offence if he intends thereby to stir up hatred or to arouse fear, or, having regard to all the circumstances, hatred is likely to be stirred up or fear is likely to be aroused thereby. However, the person is not guilty of the said offence if he did not intend to stir up hatred with his words or behaviour, or the written material, and he was not aware that his act might be, threatening, abusive, or insulting. (Article 9(4) POO)

The further articles of the POO, just as the provisions of the POA introduced in point (a) of this subchapter, state that the publishing or distributing of a written material, or distributing, showing or playing a recording of visual images or sounds is a criminal offence, if the written material or recording has threatening, abusive or insulting nature and the person committing the act intends thereby to stir up hatred or arouse fear, or, having regard to all the circumstances hatred is likely to be stirred up or fear is likely to be aroused thereby. (Articles 10(1) and 11(1) POO) Similarly, with the same characteristics, the inclusion of a programme having a threatening, abusive, or insulting nature in a programme service is also a criminal offence. In this latter case not only the person providing the programme service, but any person by whom the programme is produced or directed, and by whom offending words or behaviour are used are guilty of the mentioned offence. (Article 12(1) POO)

According to Article 13(1) POO, the possession of written material or a recording of visual images or sounds which are threatening, abusive, or insulting is a criminal offence, if the person committing the act intends or is likely to stir up hatred or arouse fear, and displays, publishes, distributes the written material, distributes, shows or plays the recording, or includes either the written material or the recording in a programme service.

¹⁶ The original text of Article 8 POO was supplemented by the terms 'sexual orientation' and 'disabled' in 2004 when the Criminal Justice (Northern Ireland) Order 2004 was adopted and amended the POO.

¹⁷ This provision was inserted by The Marriage (Same-sex Couples) and Civil Partnership (Opposite-sex Couples) (Northern Ireland) Regulations 2019. The provision is in force from 13th January 2020.

In 2020, a consultation was launched in the United Kingdom. The main goal of this consultation was to prepare the amendment of the existing regulation on hate crimes to harmonise the applicable legal consequences. The major reason for the consultation was the divergent treatment of hate crimes by criminal law. Regarding the weight of the applied legal consequences, these criminal offences were assessed differently which greatly depends on whether the offence was committed because of the belonging of the victim to a given racial group, or his disability. In practice, a demand has arisen for the extension of the criminal law regulation. According to this, beyond those characteristics that are the most common basis for hate crimes (e.g. ethnicity, racial or religious affiliation, sexual orientation, disability, transgenderism, etc.), several other personal features shall be protected which also evoke hatred within the society. Such a feature can be the person's gender (e.g. misogyny) or age (c.f. ageism), but the homelessness or the occupation (e.g. sex worker) of the person, as well as the philosophical conviction or the belonging to a subculture (e.g. gothic, punk, etc.) can also be the basis for the victimisation of hate crime.

Considering the results of the consultation, the British legislator intends to create a more efficient criminal law action against acts motivated by hatred. Acts based on discrimination on grounds of sex and gender, and racial hatred acts committed in football games would also be covered by criminal law provisions. After the close of the consultation process, the received opinions were evaluated, and a final report was published in 2021.¹⁸ The document contains detailed recommendations for the reform of hate crime offences. (E.g., among others, there is a recommendation on including the term 'asexual' into the definition of sexual orientation and replacing the term 'transgender' with the term 'transgender or gender diverse'. It is also recommended to add age as a protected characteristic in hate crime laws.)

2. Definition and regulation of cyberbullying

When researching the regulation on hate speech, the delimitation of hate speech and bullying is essential. While hate speech appears as an independent type of hate crime, bullying is not a criminal offence in the United Kingdom, even if it shows similar features. The term 'bullying' covers conduct where a person uses

¹⁸ Available at <https://assets.publishing.service.gov.uk/media/61ba053ed3bf7f055eb9b8cf/Hate-crime-report-accessible.pdf>

his power or strength to frighten or hurt someone, who is thought to be weaker. Bullying act is often performed over a longer period, and the person committing the act often forces the other person to do something he does not want to do. The scope of the victims of bullying is wide since bullying can be committed practically anywhere (e.g. school, workplace, etc.).

Compared to hate speech, which is regulated by law, the perpetration of bullying covers a much wider range of conduct. Bullying might appear in several forms of acts, independently or combined. In the case of verbal bullying, the perpetrator, the bully, uses words to hurt, harass, or scare the other person. One typical act is the use of a nickname (sobriquet) or making rude comments about the person or his family. Physical bullying always requires assault (e.g. hitting, pushing, physical abuse, aggression, etc.) Emotional abuse covers those cases where the bully wants to make an impact on the other person's emotions by using threats, making him uncertain, or displacing him from a given community (e.g. community of friends or workplace community) or a given activity (e.g. team sport).

The interception point of hate speech and bullying is discrimination since bullying also can appear as a form of discrimination when the bullying conduct (threatening or harassment) is based on the person's disability, racial or religious belonging, philosophical belief, sexual or gender identity.

As online platforms and technologies recently came to the fore, bullying appears more and more visibly in the online space, especially in social media. Bullying conduct committed in the online space is called cyberbullying by the literature. The term refers to the place of perpetration and, at the same time, distinguishes itself from the traditional, face-to-face bullying acts. Cyberbullying can be defined as an intentional aggressive behaviour involving a power imbalance between those involved, where the perpetrator, the cyberbully intends to harass, intimidate, and threaten the cyber-victim repeatedly over time using the internet (including social networking sites) and via electronic devices, such as sending text messages, emails, and video messages.¹⁹

Cyberbullying, by its nature, is particularly common among young people. According to a national survey in 2014²⁰, 42% of youth under age 25 have already felt threatened in the online space, while 56% of the asked persons have already witnessed online harassment.

The act can be committed either by computer, mobile, tablet, or game console. Cyberbullying can be realised not only via electronic correspondence (e.g.

¹⁹ El Asam and Samara, 2016, pp. 127–141; Marczak and Coyne, 2010, pp. 182–193.

²⁰ Cyberbullying: An analysis of data from the Health Behaviour in School-aged Children (HBSC) survey for England, 2014.

by sending threatening or harassing e-mails) or text messages but also by making offensive comments on social media platforms (e.g. Facebook, Twitter, Instagram, etc.) or by sharing embarrassing or smear photos or videos or making false profiles. Bullying also can take place in chat rooms, interactive video game communities (e.g. by sending messages, displacing from the game, etc.), and several other places in the online space.

Cyberbullying commonly appears not as an independent cyber act but as the supplementary or accompanying conduct of the personal, direct, and face-to-face bullying act. However, while bullying is limited to the time that the harmed person spends in the place of the commitment of the act (i.e. at school, workplace, or in another community), in the case of cyberbullying the harming conduct can be realised at any time of the day due to the unlimited availability of the Internet. A further difference is that cyberbullying, regardless of the intent of the perpetrator, typically takes place in front of a wider audience (e.g. a smear photo reaches much more people through multiple sharing). Nevertheless, proof of cyberbullying is easier in many cases since victims can take screenshots, save photos or videos, and deliver the website address to the investigating authorities. On the other hand, however, perpetrators may easily hide their identity by making themselves anonymous, and they often behave in such a way that they would never do in real life. Since in the online sphere, perpetrators do not see the reactions of their victims, they can remain emotionally almost fully independent because they are not aware of the emotional impact of their conduct, and therefore, it is more difficult for them to give up their harming activity.

As it was mentioned above, bullying including cyberbullying as a type of bullying regarding the place of perpetration, is not an independent criminal offence in the UK when finishing the manuscript of this chapter. Therefore, there is no specific law addressing conduct which can be deemed as cyberbullying. Nevertheless, due to the diversity of perpetrating conduct, various legislative provisions can be applied to both forms of bullying. In the following, these provisions are reviewed.

It also should be added that in the UK, the need for a single set of rules covering unlawful conduct committed in the online space has been growing over the last decade. In 2019, the UK Government launched a consultation²¹ on online harms to tackle internet-related risks, such as cyberbullying, and to develop a single regulatory framework that would provide a transparent set of requirements

21 The materials related to the consultation, including the White Paper on which it is based (Online Harms White Paper) and a summary of the government's responses to the consultation are available at: <https://www.gov.uk/government/consultations/online-harms-white-paper>

for ISPs to establish and maintain online safety and would ensure the protection of users' rights to free expression. The launching of this consultation was the first step in the process whose main objective was to amend and make more consistent and transparent the then-existing, rather fragmented legislation, which contains both public and private law provisions.

After the closing and the evaluation of the consultation, on 12th May 2021, the Government submitted the Draft Online Safety Bill.²² After its publication, the bill was highly criticised all over the UK and provoked debates from both theoreticians and practitioners.²³ Some critics argued that the bill was not strict enough, while others said it went too far. Some also questioned the practical applicability of some of the provisions of the bill. However, after numerous refinements, amendments, and additions, the bill was finally adopted during the parliamentary session 2022-2023. The new act entitled Online Safety Act 2023 (hereinafter OSA)²⁴ received Royal Assent on 26th October 2023. The provisions of the OSA will enter into force gradually.²⁵ Therefore, at the end of this point of the Chapter, the new criminal offences introduced by the OSA will also be reviewed, since these offences can also be committed electronically, i.e. in the online space.

According to Article 1(1) of the Protection from Harassment Act 1997²⁶, it is a criminal offence if a person pursues a conduct that amounts to the harassment of another, and which he knows or must know amounts to harassment of the other. In the online space, this conduct can be perpetrated by sending a mass of e-mails or messages with abusive content if the perpetrator intends to intimidate the other person or to cause pain and suffering for him.

Beyond the Protection from Harassment Act 1997, provisions of the Malicious Communications Act 1988²⁷ (hereinafter MCA) also can be applied to bullying. MCA declares that any person who sends to another person a letter, an electronic communication, or an article of any description that conveys a message that is indecent or grossly offensive, a threat, or information that is false and known or believed to be false by the sender, or any article or electronic communication which is, in whole or part, of an indecent or grossly offensive nature, is guilty of an offence. Furthermore, the perpetrator is required to intend by the sending of these items to cause distress or anxiety to the recipient or to any other

22 Available at https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985033/Draft_Online_Safety_Bill_Bookmarked.pdf

23 Coe, 2022, pp. 50–75; Trengove et al., 2022; Anderson, 2022.

24 Available at <https://www.legislation.gov.uk/ukpga/2023/50/enacted>

25 Regarding the commencement of the provisions see in detail Article 210 OSA.

26 Available at <https://www.legislation.gov.uk/ukpga/1997/40/contents>

27 Available at <https://www.legislation.gov.uk/ukpga/1988/27/contents>

person to whom the content or nature of the letter, electronic communication, or other article is communicated.²⁸ The term ‘sending’ shall be interpreted in a wide sense since it covers not only sending but delivering and transmitting.

It shall be noted that the content of the above-mentioned article will be amended by the Online Safety Act and the term used in Article 1(1)(a)(ii) and (iii), i.e. ‘threat’, and ‘information that is false and known or believed to be false by the sender’ will be repealed on 31st January 2024.

Regarding phone messages, the Telecommunications Act 1984²⁹ can be applied. Within the rules on the improper use of public telecommunication, Article 43 states that sending a message or other matter that is grossly offensive or of an indecent, obscene, or menacing character. The sending of a message is also punishable if the person commits the act to cause annoyance, inconvenience, or needless anxiety to another, and he knows the message to be false or persistently makes use, for that purpose, of a public telecommunication system.

The Communication Act 2003³⁰ supplements the provision of the Telecommunications Act 1984 and contains rules on the improper use of public electronic communications networks. According to Article 127 a person who sends using a public electronic communications network a message or other matter which is grossly offensive or of an indecent, obscene, or menacing character or causes any such message or matter to be so sent, is guilty of an offence. The person is also guilty of an offence if, to cause annoyance, inconvenience, or needless anxiety to another, he (a) sends using a public electronic communications network, a message that he knows to be false, (b) causes such a message to be sent, or persistently makes use of a public electronic communications network.

Comparing the content of the last two pieces it can be concluded that Telecommunications Act 1984 and the Communications Act 2003 make similar provisions for communications. The main difference is how the offence was committed, i.e. whether the offence was committed using public telecommunications or a public electronic communications network.

The Obscene Publication Act 1959³¹ prohibits the publication of obscene matters. According to Article 2(1) of the act, any person who, whether for gain or not, publishes an obscene article or who has an obscene article for publication for gain (whether gain to himself or gain to another)] shall be liable. Regarding the interpretation of this provision, Article 1 clarifies the terms ‘article’, ‘publish’, and ‘obscene’.

28 Article 1(1) MCA.

29 Available at <https://www.legislation.gov.uk/ukpga/1984/12/contents/enacted>

30 Available at <https://www.legislation.gov.uk/ukpga/2003/21/section/127>

31 Available at <https://www.legislation.gov.uk/en/ukpga/1964/74>

According to Article 1(2) of this act, the term ‘article’ shall be interpreted broadly. It means any description of an article containing or embodying matter to be read or looked at or both, any sound record, and any film or other record of a picture or pictures. For this Act an article shall be deemed to be obscene if its effect or (where the article comprises two or more distinct items) the effect of any one of its items is, if taken as a whole, such as to tend to deprave and corrupt persons who are likely, having regard to all relevant circumstances, to read, see or hear the matter contained or embodied in it. (Article 1(1) Obscene Publication Act 1959)

The term ‘publication’ is also interpreted broadly. A person publishes an article who distributes, circulates, sells, lets on hire, gives, or lends it, or who offers it for sale or for letting on hire. Moreover, in the case of an article containing or embodying matter to be looked at or a record, a person who shows, plays, or projects it or, where the matter is data stored electronically, transmits that data shall be deemed as who publishes the article. (Article 1(3) Obscene Publication Act 1959)³²

Some of the provisions of the POA have already been described above in the section on hate speech (section 1.8.1). However, the legislation referred to may also be relevant to cyberbullying. Under Article 5(1) of the POA, a person commits an offence if he uses threatening or abusive words or behaviour, or disorderly behaviour, or displays any writing, sign, or other visible representation which is threatening or abusive, within the hearing or sight of a person likely to be caused harassment, alarm, or distress thereby. Article 4A of the POA considers as a separate offence when any of the above-mentioned conduct is committed with the specific intent to cause the other person harassment, alarm, or distress.

In the case of committing cyberbullying conduct, Article 5 POA typically can be applied when a mobile phone is used not only to send a text message or picture but as a camera to record a video.

Cyberbullying conduct often involves hacking into the computer or online account of the victim. After hacking into the computer or online account of the victim, the perpetrator has access to the victim’s personal data, correspondence, and pictures, and can copy them. Perpetrators typically copy all these data to use them to harass or humiliate the victim. Harassment or humiliation can take place either through the publication of personal data on a public website or by the perpetrator sharing the obtained data with third parties by electronic

³² For more on judicial practice concerning publications with indecent content, see: *R v Phillip James McGuigan* (1996) 2 Cr App R (S) 253, *R v Land* (1999) QB 65, *R v GS* (2012) 2 Cr. App. R. 14, *R v Peacock* (unreported, 6 January 2011, Southwark Crown Court, London, UK).

mail (e.g. by sending an attachment) or by telephone message. This also includes cases where personal data or images are obtained by hacking into a computer or online account but are not shared with third parties in the online space, but, for example, by the printing out of the victim's e-mails or images on paper.

Cyberbullying may also be considered as anti-social behaviour, in which case the provisions of the Anti-social Behaviour, Crime, and Policing Act 2014 (hereinafter referred to as ABCPA)³³ may apply.

Under Article 2(1) ABCPA a behaviour is anti-social if it has caused or is likely to cause, harassment, alarm, or distress to any person. The conduct also has an anti-social nature if it can cause nuisance or annoyance to a person concerning that person's occupation of residential premises (e.g. social rented housing or owner-occupied dwelling), or it can cause housing-related nuisance or annoyance to any person. Part 1 of ABCPA grants specified organisations (e.g. a local authority, a housing provider, the chief officer of police for a police area, etc.) to apply to the courts for a civil injunction against any person aged 10 or over the court is satisfied, on the balance of probabilities, that the person has engaged or threatens to engage in anti-social behaviour, and the court considers it just and convenient to grant the injunction to prevent the respondent from engaging in anti-social behaviour. (Article 1(1) ABCPA)

Provisions of the Defamation Act 1996³⁴ (hereinafter DA 1996) and Defamation Act 2013³⁵ (hereinafter DA 2013) can be applied to cyberbullying acts if the publication of a statement has caused or is likely to cause serious harm to the reputation of the aggrieved party. Although either a natural person or a legal person can be in the position of a victim, the assessment of the term 'serious harm' is different. As Article 1(2) DA 2013 clarifies, harm to the reputation of a body that trades for profit is not 'serious harm' unless it has caused or is likely to cause the body serious financial loss.³⁶

If the conduct causing serious harm to the reputation of a person was made via the publication on a website, the aggrieved party may contact the website operator and request the removal of the infringing material. Detailed rules on defamation of reputation for website operators are set out in The Defamation (Operators of Websites) Regulations 2013.

33 Available at <https://www.legislation.gov.uk/ukpga/2014/12/contents/enacted>

34 Available at <https://www.legislation.gov.uk/ukpga/1996/31/contents>

35 Available at <https://www.legislation.gov.uk/ukpga/2013/26/contents/enacted>

36 For an interpretation of serious harm, see: *Cooke & Anor v MGN Ltd & Anor* (2014) EWHC 2831 (QB), *Ames v Spamhaus* (2015) EWHC 127 (QB), *Lachaux v Independent Print Ltd* (2017) EWCA Civ 1334, *Lachaux v Independent Print Ltd & Anor* (2019) UKSC 27, *Brett Wilson LLP v Persons Unknown* (2015) EWHC 2628 (QB), *Euroeco Fuels (Poland) Ltd & Ors v Szczecin and Swinoujscie Seaports Authority SA & Ors* (2018) EWHC 1081 (QB).

Nevertheless, under Article 1 DA 1996, a person committing the act causing serious harm to the reputation has a defence if he shows that he was not the author, editor, or publisher of the statement complained of, he took reasonable care about its publication, and he did not know, and had no reason to believe, that what he did caused or contributed to the publication of a defamatory statement. This defence called ‘innocent dissemination’ is also available for ISPs, however relying on this defence is more limited for them.

Recently, new legal acts were introduced in Scotland and Northern Ireland. Until the adoption of these new acts, the law of defamation in these parts of the UK was substantially the same as the law in England and Wales was, before the introduction of the DA 2013.

Defamation and Malicious Publication (Scotland) Act 2021 was introduced to modernise and simplify the existing law of defamation. According to Article 1(2) of the act, a defamatory statement is only actionable if the statement has been published by the publisher to a person who is other than the person about whom the statement is, and the publication of the statement has caused or is likely to cause serious harm to the reputation the person about whom the statement is.

As to Article 1(4), a statement about a person is defamatory if (a) it causes harm to the person’s reputation, i.e. it tends to lower the person’s reputation in the estimation of ordinary persons), (b) a reference to publishing a statement is a reference to communicating the statement by any means to a person in a manner that the person can access and understand, and (c) a statement is published when the recipient has seen or heard it.

It is important to note that contrary to DA 1996, Defamation and Malicious Publication (Scotland) Act 2021 abolishes the common law defences of innocent dissemination and establishes new defences (defence of truth, defence of publication on a matter of public interest, defence of honest opinion).

In Northern Ireland, rules on defamation are contained by the Defamation Act (Northern Ireland) 2022 which reviewed and reformed previously existing defamation laws, to ensure the balance in the protection of the right to freedom of expression, the right to protection of good name and reputation, and the right of access to justice.

On 13 November 2023, a consultation opened Defamation Act (Northern Ireland) 2022 to review how the new act has been operating. The review was published in June 2024 by the Department of Finance.³⁷

³⁷ Available at <https://www.finance-ni.gov.uk/sites/default/files/publications/dfp/Review%20of%20the%20Defamation%20Act%20%28NI%29%202022%20published.pdf>

In Part 10, the OSA contains criminal offences that relate to communication. These offences can be ranked into several groups.

The first group of offences includes false communication and threatening communication. A person commits the criminal offence of false communication if the person sends a message³⁸, the message conveys information that the person knows to be false, at the time of sending it, the person intended the message, or the information in it, to cause non-trivial psychological or physical harm to a likely audience, and the person has no reasonable excuse for sending the message. It is important that the provider of an internet service using which a communication is sent, transmitted, or published is not to be regarded as a person who sends a message, i.e. an ISP can not be the perpetrator of the criminal offence of false communication. (Article 179(1) OSA)

In the case of the criminal offence of threatening communication, the person also sends a message.³⁹ However, unlike the offence of false communication, the offence here also requires that the message conveys a threat of death or serious harm, and at the time of sending it, the person intended an individual encountering⁴⁰ the message to fear that the threat would be carried out (whether or not by the person sending the message) or was reckless as to whether an individual encountering the message would fear that the threat would be carried out (whether or not by the person sending the message). (Article 181(1) OSA) ‘Serious harm’ means serious injury amounting to grievous bodily harm, rape, assault by penetration (within the meaning of Article 2 of the Sexual Offences Act 2003) or serious financial loss. (Article 181(2) OSA)

In the next group, offences of sending or showing flashing images are included.⁴¹ These conducts, summarised as ‘cyber-flashing’, are a form of digital harassment or sexual misconduct. According to Article 183(1) OSA person commits

38 OSA provides for interpretation of the term ‘sends a message’. According to Article 182(2) OSA, a person ‘sends a message’ if the person (a)sends, transmits, or publishes a communication (including an oral communication) by electronic means, or (b)sends, or gives to an individual, a letter or a thing of any other description, and references to a message are to be read accordingly. Moreover, according to Article 182(3) OSA, a person also ‘sends a message’ if the person (a)causes a communication (including an oral communication) to be sent, transmitted, or published by electronic means, or (b)causes a letter or a thing of any other description to be sent, or given to an individual.

39 The term ‘sends a message’ is interpreted the same way as in Footnote 63.

40 According to Article 182(5) OSA, the term ‘encounter’, in relation to a message, means read, view, hear, or otherwise experience the message.

41 It is worth noting that until the adoption of the OSA, there was not clear regulation on the above-mentioned conduct in the UK. In contrast, however, the Sexual Offences (Scotland) Act 2009 includes the offence of ‘coercing a person into looking at a sexual image’ (Article 6) which can cover the cyber-flashing conduct. Cf. McGlynn and Johnson, 2021, pp. 183–184.

an offence if he (or she) sends a communication by electronic means which consists of or includes flashing images⁴², and at the time the communication is sent, it is reasonably foreseeable that an individual with epilepsy would be among the individuals who would view it, and the person sending the communication (hereinafter sender) sends it with the intention that such an individual will suffer harm as a result of viewing the flashing images. Sending a communication by electronic means which consists of or includes flashing images is also a criminal offence, if the sender believes that an individual whom the sender knows to be an individual with epilepsy, or whom the sender suspects to be an individual with epilepsy, will, or might, view it, and the sender intends that this individual will suffer harm as a result of viewing the flashing images. In addition to the fulfilment of one of these two conditions, the offence shall also be established if the sender has no reasonable excuse for sending the communication.

A person also commits an offence, he shows an individual (recipient) flashing images by means of an electronic communications device, and when showing the images he knows that recipient is an individual with epilepsy, or suspects that the recipient is an individual with epilepsy, and when showing the images, he intends that the recipient will suffer harm as a result of viewing them, and has no reasonable excuse for showing the images. (Article 183(8) OSA)

It is an important difference between the criminal offences regulated in Article 183(1) and 183(8) OSA that in the first case the exemptions listed in Article 180 (1)-(5) OSA are applicable, while it is not possible in the second case. Nevertheless, none of the above-mentioned criminal offences can be committed by a healthcare professional acting in that capacity. Another important provision is that a provider of an internet service by means of which a communication is sent, for the purposes of Article 183(1) OSA, is not to be regarded as a person who sends a communication.

According to Article 184(1) OSA, encouraging or assisting serious self-harm is a criminal offence. A person commits this offence if he does a relevant act capable of encouraging or assisting the serious self-harm of another person, and the act was intended to encourage or assist the serious self-harm of another person. A 'relevant act' can be for example a direct, in-person communication with the other person, sending, transmitting, or publishing a communication by electronic means.⁴³ It is important to note that intentionality is a prereq-

42 According to Article 183(13) OSA, the term 'flashing images' means images which carry a risk that an individual with photosensitive epilepsy who viewed them would suffer a seizure as a result.

43 The listing of acts that can be deemed as 'relevant act' in the application of the referred article of the OSA see Article 182(2) OSA.

uisite for establishing the offence, i.e. the person committing the act intend to encourage or assist the serious self-harm of the other person. On the other hand, the offence is independent of the result of the act, since the person commits an offence whether the result, i.e. the serious self-harm occurs or not.

Regarding ISPs, it shall be noted that a provider of an internet service by means of which a communication is sent, transmitted, or published is not to be regarded as a person who sends, transmits, or publishes it. (Article 184(10) OSA)

The OSA also provides for two new offences, the sending etc photograph or film of genitals and the sharing or threatening to share intimate photograph or film to be inserted into the Sexual Offences Act 2003.⁴⁴ The supplementation of this act is particularly important, since the conduct of the perpetrator can also be carried out electronically.

According to Article 66A(1) of the Sexual Offences Act 2003, a person who intentionally sends or gives a photograph (including both the negative and the positive version) or film (moving image) of any person's genitals to another person commits an offence if he intends that the other person will see the genitals and be caused alarm, distress or humiliation, or he sends or gives such a photograph or film for the purpose of obtaining sexual gratification and is reckless as to whether the other party will be caused alarm, distress or humiliation. The sending or giving include, in particular the sending of the photograph or film to another person by any means, electronically or otherwise, showing it to another person, and placing it for a particular person to find. (Article 66A(2) of the Sexual Offences Act 2003)

In the case of the criminal offence of sharing or threatening to share intimate photograph or film, according to Article 66B(1) of the Sexual Offences Act 2003, a person commits the offence, if he intentionally shares a photograph or film which shows, or appears to show, another person in an intimate state, this person does not consent to the sharing of the photograph or film, and the person sharing the photograph or film does not reasonably believe that the person who is showed in an intimate state consents. The person also commits the offence if he shares the photograph or film with the same character and the person who is showed in an intimate state does not consent to the sharing of the photograph or film, and the person shares the content with the intention of causing the other person alarm, distress or humiliation. Thirdly, the person commits the offence as well if he shares the photograph or film with the mentioned character for the purpose of him or another person obtaining sexual gratification, and the person who is showed in an intimate state does not consent and the person sharing the photograph or film does not reasonably believe that the other person consents.

⁴⁴ Cf. Article 66A-66D of the Sexual Offences Act 2003.

(Article 66B(2)-(3) of the Sexual Offences Act 2003) For each of the acts just mentioned, the result, i.e. the sharing of the photo or video, is realised. However, it is also a criminal offence, if the person does not actually share, but threatens the other person with the sharing of a photograph or film which shows, or appears to show, the other person in an intimate state, and he does it with the intention that the person who is showed in an intimate state or another person who knows him or her will fear that the threat will be carried out, or the person sharing the photo or film being reckless as to whether either of the mentioned persons will fear that the threat will be carried out. (Article 66B(4) of the Sexual Offences Act 2003)

In relation to the offences listed above, the legislation also sets out several exceptions, i.e. when the person does not commit a criminal offence with the sharing of a photograph or film which shows another person in an intimate state. These exceptions will not be reviewed in detail.⁴⁵

Considering the interpretation of the term ‘sharing’, Article 66D(2) of the Sexual Offences Act 2003 clarifies that a person ‘shares’ something if the person, by any means, gives or shows it to another person or makes it available to another person. Nevertheless, provider of an internet service by means of which a photograph or film is shared is not to be regarded as a person who shares it. (Article 66D(3) of the Sexual Offences Act 2003)

3. Regulation and prevention of bullying and cyberbullying at the workplace and at the school

3.1. Bullying and cyberbullying at the workplace

Since cyberbullying, as a specific type of bullying in the online space, can occur in many areas of everyday life, several additional sectoral laws may be applied in addition to those described above. One of the most common settings for bullying behaviour is the workplace, where online bullying is also becoming increasingly prevalent. According to a survey published in 2020, 23% of British employees have been bullied at work.⁴⁶

Although bullying including cyberbullying and harassment are two different categories, there are some similarities. e.g. both linked to the abuse of

⁴⁵ The exemptions are regulated in 66C of the Sexual Offences Act 2003.

⁴⁶ Cf. <https://www.smeloans.co.uk/blog/bullying-in-the-workplace-statistics-uk/>

power.⁴⁷ However, while harassment, whether based on a person's age, gender, gender identity, disability, marital status, pregnancy, race, religion, or sexual orientation, is dealt with by English law through complex regulation, bullying conduct disregarding the place of perpetration does not fall under the definition of harassment and therefore it is, in principle, not considered unlawful.

The need for a legal framework for harassment in the workplace has been expressed since the 1990s. In 1996, the Dignity at Work Bill was introduced in Parliament, which would have banned harassment in the workplace generally. The bill, however, was not passed.⁴⁸ In the UK, legislation that would contain explicit provisions for such offences or would allow for the prosecution of perpetrators still does not exist, but some special laws can be applied. Moreover, in the absence of an independent legal regulation on bullying in the workplace, the role of judicial practice is particularly important, especially for the development of the rules regarding this question.⁴⁹

Equality Act 2010 provides for harassment and victimisation and defines them as prohibited conduct. Article 26(1) of the act defines harassment as unwanted conduct related to a relevant protected characteristic (age, disability, gender reassignment, race, religion or belief, sex, sexual orientation), which has the purpose or effect of violating an individual's dignity or creating an intimidating, hostile, degrading, humiliating, or offensive environment for that individual. According to the case law, the Equality Act 2010 may apply to workplace bullying.⁵⁰

Under Article 2 of the Health and Safety at Work Act 1974⁵¹, employers are required to provide a safe working environment for their employees. This duty of the employer shall be ensured as far as it is reasonably practicable. If an employee becomes a victim of harassment, bullying, or cyberbullying at work, using the computer infrastructure used there, the employer breaches this obligation. Rules of the Protection from Harassment Act 1997 already referred to also can be applied, although it lays down general rules on harassment and does not contain a specific provision on harassment in the workplace. This was confirmed by the court in 2006 in *Majrowski v Guy's and St Thomas's NHS Trust*.⁵² It was held that an employee could also base a claim for compensation for workplace harassment on the provision of the Protection from Harassment Act 1997.

47 For a comprehensive treatment of the topic, see Einarsen, Hoel, Zapf and Cooper, 2020.

48 For details on the process of preparing and negotiating the bill and the reasons behind its rejection, see: Harthill, 2008, pp. 286–289.

49 Hoel, 2013, p. 65.

50 Cf. *Yeboah v Crofton*, 2002, IRLR 634.

51 Available at <https://www.legislation.gov.uk/ukpga/1974/37/contents>

52 *Majrowski v Guy's and St Thomas's NHS Trust* (2006) UKHL 34.

Regulation of workplace harassment and bullying continues to be a demand in British society. In response to this demand, the Bullying and Respect at Work Bill was introduced in the summer of 2023. The Bill provides for a statutory definition of bullying at work and contains detailed provisions relating to bullying at work, including to enable claims relating to workplace bullying to be considered by an employment tribunal. At the time of writing, the 1st reading in the House of Commons was completed.

3.2. Bullying and cyberbullying at the workplace

A school environment is also a typical place for abusive behaviours like bullying and, with the growth in the use of smart devices, cyberbullying.

In these cases, the acquired data and images are shared through a Virtual Learning Environment (VLE) in the form of a chat message or chat wall. Cyberbullying also covers the conduct when, following the hacking of a computer or online account, personal data or images are not shared with third parties or the public, but the perpetrator deletes data or documents (e.g. homework, university assignments, etc.) stored or uploaded to a shared storage space used by others, causing inconvenience to that person. In the above cases, in addition to the application of the classic privacy, confidentiality, and data protection rules and legal consequences, it is also possible to deem the conduct in question as a criminal offence under the Computer Misuse Act 1990⁵³ and, therefore, to apply the criminal consequences.

In the UK, a comprehensive reform of education was introduced in 1998. The School Standards and Framework Act 1998⁵⁴ prescribed state schools as mandatory to develop anti-bullying policies. From 2003, this provision shall also be applied to private institutions.

Article 89(1)(b) of the Education and Inspections Act 2006⁵⁵ states that the head teacher at a relevant school must determine measures to be taken to encourage good behaviour and respect for others on the part of pupils and prevent all forms of bullying among pupils. The measures determined by the head of the institution, to such extent as is reasonable, include measures to be taken to regulate the conduct of pupils at a time when they are not on the premises of the school and are not under the lawful control or charge of a member of the staff of the school. It shall be noted that this provision this legislation does not apply to independent schools.

⁵³ Available at <https://www.legislation.gov.uk/ukpga/1990/18/contents>

⁵⁴ Available at <https://www.legislation.gov.uk/ukpga/1998/31/contents>

⁵⁵ Available at <https://www.legislation.gov.uk/ukpga/2006/40/contents>

As a disciplinary penalty, the legislation allows the staff of the educational institution to confiscate certain devices (e.g. mobile phones) from pupils. The teacher may also ask the pupil to reveal the contents of the message or even the mobile phone to detect the bullying. Disciplinary action may be taken against a pupil who refuses the request.

For private schools in England and Wales, the Education (Independent School Standards) (England) Regulations 2014⁵⁶ contain provisions. Part 3 of the legislation, on the welfare, health, and safety of pupils, states that the proprietor of a school shall ensure that bullying at the school is prevented in so far as reasonably practicable, by the drawing up and implementation of an effective anti-bullying strategy.

It is important to note that the above-mentioned legislation only applies to independent schools in England and Wales, i.e. in the other parts of the UK separate provisions have been made for independent schools.

In Northern Ireland, the Education Reform (Northern Ireland) Order 1989 was the first legal act that required schools in Northern Ireland to develop and implement discipline policies. Later, Article 3 of the Education (Northern Ireland) Order 1998⁵⁷ provided for the responsibility of the Board of Governors and principals for discipline including implementing discipline policies. According to the original text of Article 3(3)(a)(ii), the management of the grant-aided school was required to encourage good behaviour and respect for others on the part of pupils. In 2003, the text was modified⁵⁸ and completed with the phrase ‘in particular, preventing all forms of bullying among pupils.’ This modified text was in force until 2016 when the Addressing Bullying in Schools Act (Northern Ireland) 2016⁵⁹ (hereinafter referred to as ABSA) was adopted.

Bullying is a core notion of the act. However, the scope of the act is limited to bullying at schools, therefore the term ‘bullying’ is interpreted as ‘bullying at school’. According to Article 1(1) ABSA, bullying behaviour includes, but is not limited to, the repeated use of any verbal, written, or electronic expression or other act, or a combination thereof, by a pupil or group of pupils against another pupil or group of pupils with the purpose of causing physical or emotional harm to the latter. It is worth noting that under ABSA only those bullying conduct are covered which are committed by pupils and against pupils. ABSA does not cover

56 Available at <https://www.legislation.gov.uk/uksi/2014/3283>

57 Available at <https://www.legislation.gov.uk/nisi/1998/1759/contents/made>

58 Article 3(a)(ii) of the Education (Northern Ireland) Order 1998 was amended by Article 19(3) of the Education and Libraries (Northern Ireland) Order 2003.

59 Available at <https://www.legislation.gov.uk/en/ni/2016/25/contents>. Although the Addressing Bullying in Schools Act (Northern Ireland) 2016 was adopted in 2016, it came into force on 1st September 2021.

acts which are committed either by a pupil or a teacher (or any other member of the staff) against another teacher, or by a teacher against a pupil. These bullying conducts shall be assessed under laws other than ABSA.

The Addressing Bullying in Schools Act (Northern Ireland) 2016 prescribes for the Board of Governors of a grant-aided school to determine the measures to be taken at the school to prevent bullying involving a registered pupil at the school. The measures can be applied by the Board of Governors, the staff of the school, or other persons not only on the premises of the school during the school day, but while the pupil travels to or from the school during the school term, while the pupil is in the lawful control or charge of a member of the staff of the school, or while the pupil is receiving educational provision arranged on behalf of the school and provided elsewhere than on the premises of the school.

In case of the occurrence of bullying, the Board of Governors of a grant-aided school shall ensure that a record is kept of all incidents of bullying or alleged bullying involving a registered pupil at the school. This record shall state (a) what, from all the circumstances, appears to be the motivation of the incident, and (b) the methods of bullying (i.e. it is committed using verbal, written, or electronic communication, any other act, or a combination of those). Regarding the motivation of the incident, Article 3(3) provides examples to which the motivation can relate. According to this article, bullying can be motivated by differences in religious belief, political opinion, racial group, age, sex, sexual orientation, or marital status, and differences between persons with a disability and persons without, such as differences between persons with dependants and persons without, persons based on gender reassignment, and persons based on pregnancy.

Considering the record on the occurrence of bullying conduct, the act prescribes the record to include information about how the incident was addressed.

In Scotland, the Schools (Health Promotion and Nutrition) (Scotland) Act⁶⁰ 2007 requires schools to promote health, including the mental, emotional, social, and physical health and well-being of children. The Education (Additional Support for Learning) (Scotland) Act 2004 provides for support for children and young people with learning difficulties, including support for children and young people who are experiencing difficulties because of bullying.⁶¹

As it was previously mentioned, a new legislation of a comprehensive nature has been adopted in the UK in October 2023. A key concern for the legislator was to ensure the fullest possible protection of children in online spaces. The OSA requires ISPs to identify, mitigate and manage the risks of harm from content

⁶⁰ Available at <https://www.legislation.gov.uk/asp/2007/15/contents/2008-08-04>

⁶¹ Available at <https://www.legislation.gov.uk/asp/2004/4/contents/2014-08-01>

and activity that is harmful to children, and to regulate. Moreover, OSA seek to secure (among other things) that services are safe by design, and designed and operated in such a way that a higher standard of protection is provided for children than for adults. (Article 1(2)-(3) OSA).

Several measures are introduced by the OSA which aimed at ensuring the online safety for children. Establishing new criminal offences is of particular importance for the protection of children, as the victims of these newly criminalised conduct under the OSA were, in the vast majority of cases, children. This will certainly mean much stronger protection for children against abusive behaviour in the online space in the future.

The OSA requires ISPs to introduce age assurance and age verification to ensure that children cannot access such services which are not designed for them (e.g. porn sites). Although users including persons under the age of 18 have always had to answer the question whether or not they are over 18, but in the future age verification will have to be done in a different and more rigorous way. Operators of social media platforms also must prevent children accessing them before the minimum age. These ISPs are obliged to take action to prevent illegal and harmful content (including images or videos of child sexual abuse and exploitation) from being shared on their social media site and making sure that the content is quickly removed.

In practice, a major problem was that parents could not access their children's online data, such as their personal account in a social media platform in the event of their child's death. In the future, under the provisions of the OSA, parents will be able to do this. Moreover, OSA provides children and their parents with a more effective toolkit for reporting online infringements.

4. Crimes committed in the online space, cyberbullying, and the enforceability of the authorities' action against hate speech

In the case of hate crimes committed in the online space and explicitly criminalised by law, criminal law consequences are applied according to the criminal procedural rules. The victim of the crime also plays an important role in the activity of the investigating authority in collecting evidence, as his report and testimony serve as primary evidence in the case. On the other hand, however, in those cyberbullying conduct which are considered a criminal offence, the process of revealing the facts and proving them is often quite difficult. Recalling

cyberbullying is often very emotionally distressing for the victim, especially in those cases where the act took place over a long time and caused the victim serious psychological distress.

As the conduct of bullying and cyberbullying are not separate criminal offences in the UK, criminal sanctions can only be applied if the act also has elements of other criminal offences. In the lack of this, the victim of the bullying or cyberbullying can at most make a compensation claim against the perpetrator for the suffered harm.

As it was noted above, acts of bullying and cyberbullying most often take place in the workplace or educational institutions. Although English law obliges the employer to ensure proper working conditions including the mental and psychological well-being of employees, bullying conduct is mostly dealt with in the workplace secretly, 'behind closed doors.' Official action is only be taken if the bullying conduct can be classified as criminal or other legal offence under a legal act, for example, if the given conduct includes the elements of harassment or, constitutes defamation at the same time.

As noted above, in the case of educational institutions there are several legal provisions aimed at preventing bullying conduct in the school or dealing with the acts that have already taken place. However, as with bullying conduct in the workplace, such acts in schools and between pupils are primarily treated at the local level, i.e. by the educational institution. The educational institution records the behaviour, its background, its real or perceived reasons, and how it is dealt with (e.g. applied consequence, disciplinary action) and provides support (e.g. access to a psychologist) to the victim of the bullying conduct if he requests it.

The perpetrators of bullying and cyberbullying conduct in educational institutions, due to their age, often cannot be held criminally liable even if their actions are criminalised. Nevertheless, in cases where the conduct can be assessed as anti-social behaviour, the measures set out in the separate act (ABCPA) may be applied to a person over 10 years of age if it can be shown that the measure is necessary to protect the person or persons harmed by the anti-social behaviour from further anti-social behaviour.

Under English law, civil enforcement, provided that the bullying or cyberbullying conduct also amounts to a violation of privacy rights, is possible, but requires prudent consideration, since the costs of such claims are relatively high.

In those cases where the infringing conduct (e.g. defamation) takes place on the Internet, the aggrieved party may contact the operator (Internet service provider, hereinafter ISP) of the website and can request the removal of the infringing content. However, Article 1 of the DA 2013, cited above, allows the ISP to

rely on the so-called ‘innocent dissemination’, but only until he becomes aware that the content published on the website may be capable of causing damage to honour or reputation.

Where the aggrieved party chooses the civil enforcement and the proceeding results in a judgment in the case, The Defamation (Operators of Websites) Regulations, also mentioned above, provide the possibility for the court to oblige the defendant (infringing party) to publish a summary of the judgment. It is worth noting, however, that in judicial practice, this type of judgment is rarely handed down.⁶²

5. The liability of internet service providers and social media platforms

Nowadays, the number of online statements that damage the social image and reputation of a person is increasing in the UK due to the growing use of social media (e.g. Facebook, Twitter). This trend poses an increasing risk to online users. Expressing the opinion in the online space and the infringements relating to them, as well as the questions that arose on the treatment of these infringements, made ISPs a key player in the problem. The regulation of the liability of ISPs and social media service providers have long been the focus of both jurisprudence and legal attention. The provisions on the liability of ISPs appear in several pieces of legislation and will be briefly discussed below, including the relevant case law.

DA 2013 contains detailed rules on the liability of ISPs for the publication of infringing content and establishes new defences for ISPs.⁶³ The liability of the operator of an Internet website depends on the identity of the person who made the infringing statement.

Article 5 DA 2013 provides a new defence for website operators considering statements posted on their sites by third parties. By relying on this, an ISP can argue that it did not post the infringing statement on its website. Where a post is uploaded to a website by an identifiable person, the existing law provides that the host will have a defence only in the absence of knowledge on their part of the defamatory statement. The person who posted the statement can be identified

62 On the publication of the summary of the judgment see *Shakil-Ur-Rahman v ARY Network Ltd* (2016) EWHC 3110 (QB), *Turley v UNITE the Union & Anor* (2019) EWHC 3547., *Monir v Wood* (2018) EWHC 3525 (QB).

63 Mullis et al., 2013.

if the aggrieved party has sufficient information to bring proceedings against that person.

Accordingly, the ISP cannot be exempted from liability, even if the defence was invoked, if the aggrieved party proves that (a) the person who posted the statement with the infringing content on the website was not identifiable, (b) he or she gave a notice of complaint to the ISP concerning the statement, (c) and the ISP failed to respond to the notice of complaint of the aggrieved party. Although the primary aim of the DA 2013 was to protect persons against defamation, the law tips the balance in favour of freedom of expression and protection against defamation.

Additional protection for ISPs can be found in Article 10 DA 2013, which states that a court has no jurisdiction to hear and determine an action for defamation brought against a person who was not the author, editor, or publisher of the statement complained of unless the court is satisfied that it is not reasonably practicable for an action to be brought against the author, editor, or publisher.

The previous but still existing law on defamation, i.e. DA 1996, also contains a defence by which the person can be exempted from liability. According to Article 1 of the DA 1996, a person has a defence if he proves that he was not the author, editor, or publisher of the statement complained of, he took reasonable care concerning its publication, and he did not know, and had no reason to believe, that his conduct would result in or contribute to the publication of a defamatory statement. Since there is no specific mention of an ISP in the DA 1996, it was the judicial practice that designed the framework of the defence for ISPs. (Relating judgments will be referred to in point c) of this subheading.)

In Scotland, the Defamation and Malicious Publication (Scotland) Act 2021 provides for ISPs. In Article 3, there is a restriction on proceedings against secondary publishers which provides that there is no right to bring defamation proceedings against a person about a statement in Scotland unless they are the author, editor, or publisher of the statement.⁶⁴ The act does not contain a corresponding defence specifically for ISPs in Scotland, though they can be protected by other defences. Therefore, defences in Scotland and England are not identical, but they will likely overlap in their operation.

⁶⁴ In the application of Article 3, ‘author’ means the person from whom the statement originated, but does not include a person who did not intend the statement to be published, ‘editor’ means a person with editorial or equivalent responsibility for the content of the statement or the decision to publish it, and ‘publisher’ means a commercial publisher (that is to say, a person whose business is issuing material to the public or to a section of the public) who issues material containing the statement in the course of that business.

The Defamation (Operators of Websites) Regulations 2013 also contains rules concerning the liability of ISPs. Regulation 3 and the Schedule provide for the actions to be taken by the operator in response to the notice of the aggrieved party to maintain Article 5(2) defence.

In 2002, the e-Commerce Directive of the European Union⁶⁵ was implemented by The Electronic Commerce (EC Directive) Regulations which contains the same rules on the liability of ISPs as Section 4 of the e-Commerce Directive. The Electronic Commerce (EC Directive) Regulations 2002 determines three cases, the so-called safe harbours (mere conduit, caching, and hosting) where the provider may be exempted from liability.

Regarding the case of mere conduit, Article 17(1) of The Electronic Commerce (EC Directive) Regulations 2002 states that in those cases where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service or the provision of access to a communication network, the service provider (if he otherwise would) shall not be liable for damages or for any other pecuniary remedy or any criminal sanction as a result of that transmission where the service provider (a) did not initiate the transmission, (b) did not select the receiver of the transmission, and (c) did not select or modify the information contained in the transmission. The acts of transmission and provision of access include the automatic, intermediate, and transient storage of the information transmitted where this takes place for the sole purpose of carrying out the transmission in the communication network, and the information is not stored for any period longer than is reasonably necessary for the transmission.

Article 18(1) of The Electronic Commerce (EC Directive) Regulations 2002 provides about caching. Where an information society service is provided which consists of the transmission in a communication network of information provided by a recipient of the service, the service provider (if he otherwise would) shall not be liable for damages or any other pecuniary remedy or for any criminal sanction as a result of that transmission where the information is the subject of automatic, intermediate and temporary storage where that storage is for the sole purpose of making more efficient onward transmission of the information to other recipients of the service upon their request. Further requirements for the defence are that the service provider

- does not modify the information,
- complies with conditions on access to the information,

⁶⁵ 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, pp. 1–16.

- complies with any rules regarding the updating of the information, specified in a manner widely recognised and used by the industry,
- does not interfere with the lawful use of technology, widely recognised, and used by industry, to obtain data on the use of the information, and
- acts expeditiously to remove or to disable access to the information he has stored upon obtaining actual knowledge of the fact that the information at the initial source of the transmission has been removed from the network, or access to it has been disabled, or that a court or an administrative authority has ordered such removal or disablement.

According to Article 19(1) of The Electronic Commerce (EC Directive) Regulations 2002, ISP shall not be liable for damages or for any other pecuniary remedy or for any criminal sanction, if the information society service provided by the ISP consists of the storage of information (hosting) provided by a recipient of the service, and the ISP does not have actual knowledge of unlawful activity or information and, where a claim for damages is made, is not aware of facts or circumstances from which it would have been apparent to the service provider that the activity or information was unlawful, or upon obtaining such knowledge or awareness, ISP acts expeditiously to remove or to disable access to the information. A further requirement is for exempting from liability that the recipient of the service was not acting under the authority or the control of the ISP.⁶⁶

The liability of ISPs has been the subject of several judgments in English case law. In this respect, the assessment of ISPs is rather controversial. There have been cases where the liability of the ISP was established because the court did not see the applicability of the exemption under Article 1 of the DA 1996.⁶⁷ In other cases, the activity of the service provider was assessed as a simple data transfer (mere conduit) and therefore it was exempted from liability.⁶⁸ If an ISP appears only as a passive medium of communication, it cannot be considered as a publisher of data or information. This was also confirmed by the court in the Google case where it was considered that Google as a search engine is not a

⁶⁶ For case law on the application of the Article 19 exemption see *Karim v Newsquest Media Group* (2009) EWHC 3205 (QB), *Kaschke v Gray* (2010) EWHC 690 (QB), *Davison v Habeeb* (2011) EWHC 3031 (QB), *Tamiz v Google* (2012) EWHC 449 (QB), *McGrath v Dawkins* (2012) EWHC B3 (QB), *McAlpine v Bercow* (2013) EWHC 1342 (QB), *Cairns v Modi* (2012) EWCA Civ 1382.

⁶⁷ *Godfrey v Demon Internet Limited* (1999) EWHC QB 240. The case is described and analysed in detail by Michael Deturbide. See Deturbide, Michael: Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses, In: *The Journal of Information, Law, and Technology*, No. 3/2000.

⁶⁸ *Totalise Plc v Motley Fool Ltd.* [2001] EWHC 706 (QB), *Bunt v Tilley* (2006) EWHC 407 (QB).

publisher at common law. It merely provides the framework for people to search for information on the Internet but cannot filter out previously infringing content. Therefore, the liability of Google as a search engine was not established.⁶⁹ It is important to note that the search engine operator cannot be held liable even if it has already been notified about the existence of the infringing content. Similarly, the liability of the service provider for content that has already been archived and is in the fragmented list has also not been established.⁷⁰ To sum up, in English law, search engine operators enjoy complete immunity from the application of the rules on liability for internet content that negatively affects public perception.

Recently, the role of an ISP as a blog operator was also discussed in judicial practice. There is a judgment where the court did not accept Google's reference to Article 1 of DA 1996.⁷¹ In another case, the court took the opposite position and did not find Google liable for defamation.⁷² However, this decision was reversed by the Court of Appeal who held that Google knew about the publication of the defamatory statement, since it received the notice. Therefore, Google cannot successfully rely on the defence based on Article 1 DA 1996 and is liable for defamation.⁷³

Reviewing the English regulation and case law on the liability of ISPs, it can be stated that the question of determining liability remains rather uncertain; drawing the line between the mere transmission of data and the provision of content is still difficult. This is also reflected in the judgments given in the cases against Google. While the activity of Google as a search engine was considered by the court as a simple data transfer, and therefore, it was not found liable, its activity as a blog operator was found to be actionable after the notification of the infringing content.

The adoption of the OSA in October 2023, by the reshaping of their responsibilities, has significant impact on the regulation of the operation of ISPs. As it is declared in the introduction of the OSA, it provides for a new regulatory framework which has the general purpose of making the use of internet services regulated safer for individuals in the UK. To achieve this purpose, the OSA requires service providers to identify, mitigate, and manage the risks of harm from illegal content and activity, and content and activity that is harmful to children. Moreover, the OSA confers new functions and powers to the Office of

69 Metropolitan International Schools Ltd v Designtecnica Corp. (2009) EWHC 1765 (QB).

70 Budu v BBC (2010) EWHC 616 (QB).

71 Davison v Habeeb (2011) EWHC 3031 (QB).

72 Tamiz v Google (2012) EWHC 449 (QB).

73 Tamiz v Google (2013) EWCA Civ 68.

Communications (hereinafter OFCOM) which is the UK communications regulator, overseeing the broadcasting, telecommunications, and postal industries. (Article 1(2) OSA)

Provisions of the OSA, on the one hand, cover online service providers that allow people to create or share content or interact with each other. In the wording of the legislation, these are the ‘user-to-user services’ where the content is generated directly on the service by a user of the service or uploaded to or shared on the service by a user of the service and may be encountered by another user, or other users, of the service. (Article 3(1) OSA). Accordingly, these services include various social media services, photo- and video-sharing services, services facilitating chat, and other forms of direct communication, as well as online and mobile gaming services. On the other hand, ‘search services’, i.e. internet services that are, or include, a search engine, are also covered by the regulation. (Article 3(4) OSA) Beyond the providers of user-to-user services and service services, OSA regulates certain online pornographic content as well.

It is important to note that the regulation applies to all online service providers, regardless of their size, i.e. provisions of the OSA shall also be applied for individuals who provide an online service.

The duty of care of the ISPs is in the core of the new regulation. Part 3 OSA imposes duties of care separately on providers of user-to-user services (Chapter 2) and search services (Chapter 3). Certain duties of care relate to the content (illegal content) or activity of the service providers, while others are established regarding services which are likely to be accessed by children (Chapter 4), or relating to fraudulent advertising (Chapter 5). Moreover, the OSA clearly designates the borders within OFCOM can act free and, at the same time, requires OFCOM to issue codes of practice about the duties of care of the service providers (Chapter 6). In 2024, OFCOM published the Illegal content Codes of Practice for user-to-user services⁷⁴ and the Illegal content Codes of Practice for search services.⁷⁵ Depending on the completion of the Parliamentary process of these codes, from 17 March 2025, providers will have to take the safety measures set out in the Codes of Practice or use other effective measures to protect users from illegal content and activity.

74 <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-user-to-user-services.pdf?v=387711>

75 <https://www.ofcom.org.uk/siteassets/resources/documents/online-safety/information-for-industry/illegal-harms/illegal-content-codes-of-practice-for-search-services.pdf?v=387710>

Bibliography

- Anderson, R., Gilbert, S. (2022) ‘*The Online Safety Bill. Policy Brief*’, October; <https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/09/Policy-Brief-Online-Safety-Bill.pdf>
- Bleich, E. (2018) From Race to Hate: ‘A Historical Perspective’ in Brudholm, Thomas – Schepelehn Johansen, Brigitte (eds.): *Hate, Politics, Law: Critical Perspectives on Combating Hate*, Oxford University Press, Oxford, pp. 15–33
- Bleich, E. (2011) ‘The Rise of Hate Speech and Hate Crime Laws in Liberal Democracies’, *Journal of Ethnic and Migration Studies*, Vol. 37, No. 6, July, pp. 917–934
- Bechtold, E. (2022) ‘Scotland’s New Hate Crime Act Imperils Freedom of Expression’, *The Edinburgh Law Review*, Vol. 26, No. 2, pp. 250–257
- Coe, P. (2023) ‘Assessing damages for intentional infliction of harm, misuse of private information and breach of confidence in ‘image-based abuse’ claims’, *Professional Negligence*, Vol. 39, Issue 3, pp. 137–141
- Coe, P. (2023) ‘Tackling online false information in the United Kingdom: The Online Safety Act 2023 and its disconnection from free speech law and theory’, *Journal of Media Law*, Vol. 15, Issue 2, pp. 213–242
- Coe, P. (2022) ‘The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora’s box?’, *Journal of Media Law*, Vol. 14, Issue 1: The regulation of hate speech online, pp. 50–75
- Cumper, P. (2006) ‘Outlawing incitement to religious hatred – a British perspective’, *Religion and Human Rights*, Vol. 1, No. 3, pp. 249–268
- Deturbide, M. (2000) ‘Liability of Internet Service Providers for Defamation in the US and Britain: Same Competing Interests, Different Responses’, *The Journal of Information, Law, and Technology*, No. 3
- Edge, P. W. (2018) ‘Oppositional Religious Speech: Understanding Hate Preaching’, *Ecclesiastical Law Journal*, Volume 20, Issue 3, pp. 278–289
- Einarsen, S. V., Hoel, H., Zapf, D., Cooper, C. L. (2020) ‘The Concept of Bullying and Harassment at Work’, in Einarsen, S. V. et al. (eds.): *Bullying and Harassment in the Workplace. Theory, Research and Practice*, CRC Press, Boca Raton, pp. 3–39
- El Asam, A., Samara, M. (2016) ‘Cyberbullying and the law: A review of psychological and legal challenges’, *Computers in Human Behaviour*, Vol. 65, December, pp. 127–141
- Foster, S. (2019) ‘Accommodating Intolerant Speech: Religious Free Speech versus Equality, and Diversity’, *European Human Rights Law Review*, No. 6, pp. 609–625

- Goodall, K. (2009) 'Challenging hate speech: incitement to hatred on grounds of sexual orientation in England, Wales and Northern Ireland', *The International Journal of Human Rights*, Vol. 13, Issue 2-3, pp. 211-232
- Goodall, K. (2007) 'Incitement to Religious Hatred: All Talk and no Substance?', *The Modern Law Review*, Vol. 70, No. 1, January, pp. 89-113
- Hare, I. (2006) 'Crosses, Crescents and Sacred Cows. Criminalising Incitement to Religious Hatred', *Public Law*, 3, pp. 521-538
- Harthill, S. (2008) 'Bullying in the Workplace: Lessons from the United Kingdom', *Minnesota Journal of International Law*, Vol. 17, Issue 2, pp. 247-302.
- Hoel, H. (2013) 'Workplace Bullying in United Kingdom', *Workplace Bullying and Harassment*, No. 2, pp. 61-76
- Johnson, V. R. (2016) 'Comparative Defamation Law: England and the United States', *University of Miami International and Comparative Law Review*, Vol. 24, Issue 1, pp. 1-97
- Marczak, M., Coyne, I. (2010) 'Cyberbullying at school: Good practice and legal aspects in the United Kingdom', *Australian Journal of Guidance and Counseling*, Vol. 20, No. 2, pp. 182-193.
- McGlynn, C., Johnson, K. (2021) 'Criminalising Cyberflashing: Options for Law Reform', *The Journal of Criminal Law*, Vol. 85, No. 3, pp. 171-188
- McGuire, K., Salter, M. (2014) 'Legal Responses to Religious Hate Crime: Identifying Critical Issues', *Kings Law Journal*, Vol. 25, Issue 2, pp. 159-184
- Mullis et al. (2013) A comprehensive description and analysis of the new defences established by DA 2013, pp. 1-97.
- Mullis, A., Scott, A. (2014) 'Tilting at Windmills: the Defamation Act 2013', *The Modern Law Review*, Vol 77, No. 1, pp. 87-109
- Neller, J. (2023) 'Race, religion, law: an intertextual micro-genealogy of 'stirring up hatred' provisions in England and Wales', *Critical Discourse Studies*, Vol. 2020, No. 3, pp. 282-293, p. 285
- Thompson, S. (2012) 'Freedom of expression and hatred of religion', *Ethnicities*, Vol. 12, Issue 2, pp. 215-232
- Trengove, M., Kazim, E., Almeida, D., Hilliard, A. Zannone, S. Lomas, E. (2022) 'A critical review of the Online Safety Bill', *Patterns*, Vol 3, Issue 8
- Vaughan, M. (2019) 'Accepting the 'D' word: discrimination in 1960s' UK academic discourse', *Race & Class*, Vol. 61, pp. 85-95

XVI. NEW CHALLENGES, NEW LAWS: TACKLING HATE CRIMES AND CYBERBULLYING IN IRELAND

ATTILA HORVÁTH

1. The legal dimensions of hate speech and hate crime

1.1. The 1989 Prohibition of Incitement to Hatred Act and its critics

Ireland has had a specific law prohibiting hate speech since 1989.¹ The scope of the *Prohibition of Incitement To Hatred Act 1989* (hereinafter: PIHA) is not limited to hate speech in the narrow sense. Considered progressive at the time of its adoption,² the drafting of the PIHA, which some consider to be ahead of its time,³ was motivated by international obligations, notably the *International Covenant on Civil and Political Rights* (ICCPR) and the 1965 *International Convention on the Elimination of All Forms of Racial Discrimination*, and by a general consensus on the need for a domestic law, irrespective of international obligations, in particular, to combat racially motivated incitement.⁴

The first element of the PIHA (Actions likely to stir up hatred) reads as follows:

2.—(1) It shall be an offence for a person—

1 It should be noted here that Ireland does not have a single criminal code covering both the general section and the specific offences. Instead, a combination of different laws and court decisions form the basis of substantive criminal law.

2 Schweppe et al., 2014, footnote 30 at p. 17.

3 Schweppe and Walsh, 2008, p. 56.

4 Cowhey, 2006, p. 35.

- (a) to publish⁵ or distribute⁶ written material,⁷
- (b) to use words, behave or display written material—
 - (i) in any place other than inside a private residence,⁸ or
 - (ii) inside a private residence so that the words, behaviour or material are heard or seen by persons outside the residence,
- or
- (c) to distribute, show or play a recording⁹ of visual images or sounds, if the written material, words, behaviour, visual images or sounds, as the case may be, are threatening, abusive or insulting and are intended or, having regard to all the circumstances, are likely to stir up hatred.¹⁰

According to the law, ‘hatred’ means hatred against a group of persons in the State or elsewhere on account of their race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation.¹¹

Under certain circumstances, the offender may be exempted from criminal responsibility:

-
- 5 ‘Publish’ means publish to the public or a section of the public and cognate words shall be construed accordingly [PIHA, Section 1(1)].
 - 6 ‘Distribute’ means distribute to the public or a section of the public and cognate words shall be construed accordingly [PIHA, Section 1(1)].
 - 7 ‘Written material’ includes any sign or other visual representation [PIHA, Section 1 (1)].
 - 8 ‘Private residence’ means any structure (including a tent, caravan, vehicle, vessel or other temporary or moveable structure) or part of such a structure used as a dwelling but does not include any part not so used or any part in which a public meeting is being held; and in this definition ‘public meeting’ means a meeting at which the public are entitled to be present, on payment or otherwise and as of right or by virtue of an express or implied permission [PIHA, Section 2(3)].
 - 9 ‘Recording’ means any record from which visual images or sounds may, by any means, be reproduced, and references to the distribution, showing or playing of a recording are to its distribution, showing or playing to the public or a section of the public and ‘distribute’, ‘show’ and ‘play’, and cognate words, in relation to a recording, shall be construed accordingly [PIHA, Section 1 (1)].
 - 10 For an evaluation of the provision, see Schweppe and Walsh, 2008, pp. 61–64. It should be noted that during the legislative process, it was suggested that ‘ridicule’ and ‘contempt’ should be criminalised, but the Minister of Justice resisted on the grounds that that would be too severe an encroachment on freedom of expression (Schweppe and Walsh, 2008, p. 59).
 - 11 PIHA, Section 1(1). It should be noted, however, that the term ‘hate’ itself is not defined in the PIHA, as critics of the Act have pointed out (e.g. Cowhey, 2006, p. 40; Schweppe and Walsh, 2008, p. 60). A possible definition of hate speech: ‘abusive speech that targets members of certain groups—typically minority groups—including racial groups, ethnic groups, religious groups, groups defined on the basis of sexual orientation and so on’ (Harel, 2021, p. 455.),

- (2) (a) In proceedings for an offence under subsection (1), if the accused person is not shown to have intended to stir up hatred, it shall be a defence for him to prove that he was not aware of the content of the material or recording concerned and did not suspect, and had no reason to suspect, that the material or recording was threatening, abusive or insulting.
- (b) In proceedings for an offence under subsection (1) (b), it shall be a defence for the accused person—
 - (i) to prove that he was inside a private residence at the relevant time and had no reason to believe that the words, behaviour or material concerned would be heard or seen by a person outside the residence, or
 - (ii) if he is not shown to have intended to stir up hatred, to prove that he did not intend the words, behaviour or material concerned to be, and was not aware that they might be, threatening, abusive or insulting.

The second element is based on the broadcasts¹² likely to stir up hatred.

- 3.—(1) If an item involving threatening, abusive or insulting visual images or sounds is broadcast, each of the persons mentioned in subsection (2) is guilty of an offence if he intends thereby to stir up hatred or, having regard to all the circumstances, hatred is likely to be stirred up thereby.
- (2) The persons referred to in subsection (1) are:
 - (a) the person providing the broadcasting service concerned,
 - (b) any person by whom the item concerned is produced or directed, and
 - (c) any person whose words or behaviour in the item concerned are threatening, abusive or insulting.¹³

In many cases, the law exempts the offender from criminal liability.

- (3) In proceedings against a person referred to in *paragraph (a) or (b) of subsection (2)* for an offence under this section, if the person is not shown to have intended to stir up hatred, it is a defence for him to prove—
 - (a) that he did not know and had no reason to suspect that the item concerned would involve the material to which the offence relates, or
 - (b) in a case other than one to which *paragraph (a)* relates, that, having regard to the circumstances in which the item was broadcast, it was

¹² ‘Broadcast’ means the transmission, relaying or distribution by wireless telegraphy or by any other means or by wireless telegraphy in conjunction with any other means of communications, sounds, signs, visual images or signals, intended for direct reception by the general public whether such communications, sounds, signs, visual images or signals are actually received or not [PIHA, Section 1(1)].

¹³ For an evaluation of the provision, see Schweppe and Walsh, 2008, pp. 64–66.

not reasonably practicable for him to secure the removal of the material aforesaid.

- (4) In proceedings against a person referred to in *subsection (2) (b)* for an offence under this section, it is a defence for the person to prove that he did not know and had no reason to suspect—
 - (a) that the item would be broadcast, or
 - (b) that the circumstances in which the item would be broadcast would be such that hatred would be likely to be stirred up.
- (5) In proceedings against a person referred to in *subsection (2) (c)* for an offence under this section, it is a defence for the person to prove that he did not know and had no reason to suspect—
 - (a) that an item involving the use of the material to which the offence relates would be broadcast, or
 - (b) that the circumstances in which such an item would be broadcast would be such that hatred would be likely to be stirred up.
- (6) In proceedings for an offence under this section, it is a defence for the person charged to prove that he did not know, and had no reason to suspect, that the material to which the offence relates was threatening, abusive or insulting.

The third element of the law is related to the preparation and possession of material likely to stir up hatred.

4.—(1) It shall be an offence for a person—

- (a) to prepare or be in possession of any written material with a view to its being distributed, displayed, broadcast or otherwise published, in the State or elsewhere, whether by himself or another, or
- (b) to make or be in possession of a recording of sounds or visual images with a view to its being distributed, shown, played, broadcast or otherwise published, in the State or elsewhere, whether by himself or another, if the material or recording is threatening, abusive or insulting and is intended or, having regard to all the circumstances, including such distribution, display, broadcasting, showing, playing or other publication thereof as the person has, or it may reasonably be inferred that he has, in view, is likely to stir up hatred.¹⁴

Section 4(2) provides for a number of defences in proceedings concerning an alleged offence under the section.

¹⁴ For an evaluation of the provision, see Schweppe and Walsh, 2008, pp. 66–68.

(2) In proceedings for an offence under this section, if the accused person is not shown to have intended to stir up hatred, it shall be a defence for him to prove that he was not aware of the content of the material or recording concerned and did not suspect, and had no reason to suspect, that the material or recording was threatening, abusive or insulting.

It should be noted here that the regulation of online media did not arise at the time of the adoption of the PIHA, but the Department of Justice and Equality’s 2019 public consultation on the review of the Act highlighted that ‘The wording of the 1989 Act is broad enough to cover incitement via modern technologies and online behaviour. The definitions of “broadcast”, “publish”, “recording” and “distribute” in the Act are wide enough to cover online broadcasting, publication and social media discourse’.¹⁵

Under the PIHA, legal persons may also be held criminally liable if the offences covered by the Act are committed by corporate bodies:

7.—(1) Where an offence under this Act has been committed by a body corporate and is proved to have been committed with the consent or connivance of or to be attributable to any neglect on the part of a person being a director, manager, secretary or other similar officer of the body corporate, or a person who was purporting to act in any such capacity, that person as well as the body corporate shall be guilty of an offence and shall be liable to be proceeded against and punished as if he were guilty of the first-mentioned offence.

Since the 2000s, the PIHA has come under criticism from several directions. Keogh even called the law a ‘paper tiger’, referring to its questionable effectiveness.¹⁶ In particular, the author criticised the phrase ‘having regard to all the circumstances, are likely to stir up hatred’, which, in his view, implies that the classification of the conduct at issue will depend upon the character of the person(s) *to whom the hateful communication is directed*.¹⁷ Keogh illustrated this with the following example: it is unlikely that a racist pamphlet is capable of foment hatred amongst ‘most right-minded citizens’, but material or speeches aimed at confirmed racists may be the subject of prosecution as their hatred is likely to increase or be reinforced. The author has also proposed removing the phrase ‘are threatening, abusive or insulting’, as this would allow the incitement offence

¹⁵ Department of Justice and Equality, 2019, p. 5.

¹⁶ Keogh, 2000.

¹⁷ Keogh, 2000, p. 180.

to encompass many of the more ‘subtle and sophisticated’ manifestations of hate speech.¹⁸

Cowhey’s objection in principle to the PIHA was that it approached the problem from the point of view of restricting freedom of expression. He argued that it would be more appropriate for the legislature – and thus the law enforcer – to regard incitement to hatred as a matter of public order. (He used the term ‘public order legislation’.) Cowhey claimed about PIHA, that ‘the major disadvantage of such legislation is that it can polarise sections of society, creating divisions because of the way in which racist abuse is dealt with’. Furthermore, he asserted that while various minority groups are interested in being protected from the threat of racist abuse, other parts of society (although they may agree with this aim) do not want to sacrifice their right to free speech.¹⁹ Cowhey also pointed out that ‘Another disadvantage of prosecutions under specific hate speech laws is that they politicise such prosecutions, giving the “oxygen of publicity” to those who espouse racist views’.²⁰ In his view, public order legislation would limit freedom of speech to a less overt (and far less controversial) extent than laws designed specifically to prevent hate speech – and restrictions on speech on public order grounds are more widely accepted.²¹

To illustrate the effectiveness of the PIHA, Cowhey also recalled that between 1989 and 2000 there were no successful prosecutions under the Act, and although prosecutions increased in later years, there were still only a few convictions.²² He argued that ‘the more specific the law is in relation to penalising hate speech, the more difficult it is to prosecute an offender, given the political implications and balancing of rights that such a prosecution entails’.²³ The author considered that prosecution under section 6(1)²⁴ of the *Criminal Justice (Public Order) Act 1994* may be more effective, ‘because there is no need to show that the behavior was intended or likely to stir up hatred; all that has to be shown is that the behavior was threatening, abusive or insulting in a public place with intention or recklessness as to whether a breach of the peace would

18 Keogh, 2000, p. 181.

19 Cowhey, 2006, p. 41.

20 Cowhey, 2006, p. 41.

21 Cowhey, 2006, p. 42.

22 Government of Ireland, 2004, p. 36. In 2017, the Irish Courts Service revealed that there had been 44 prosecutions and five convictions under the PIHA since 2000 (Gallagher, 2017, cited in Sweeney and Farmer, 2022, p. 23.).

23 Cowhey, 2006, p. 38.

24 Threatening, abusive or insulting behaviour in public place – ‘It shall be an offence for any person in a public place to use or engage in any threatening, abusive or insulting words or behaviour with intent to provoke a breach of the peace or being reckless as to whether a breach of the peace may be occasioned.’

be caused'.²⁵ Overall, Cowhey concluded that the PIHA has not proved effective in enforcing the obligations imposed by the two international conventions. In his view, there is a 'reluctance to use the Act at all' due to the difficulty in prosecuting offenders.²⁶

Schweppe and Walsh pointed out that at the time of the enactment of the PIHA, it was not widely believed that racially motivated hatred was a general problem in Ireland, so 'the Act was conceived as a minimalist measure designed to meet the requirements of Article 20(2) of the ICCPR', which states that 'Any advocacy of national, racial or religious hatred that constitutes incitement to discrimination, hostility or violence shall be prohibited by law'.²⁷ The authors identified several problematic points in the PIHA. Firstly, they claimed that the terms 'abusive' and 'insulting' have a more extensive and ill-defined scope, and the very existence of such broadly defined offences can have a chilling effect on the freedom of debate and the freedom to express one's views.²⁸ On the other hand, it has been held that the PIHA does not apply if, for example, a racist verbal insult is inappropriate for hate speech in the circumstances.²⁹

Taylor noted that the PIHA 'has a very specific and narrow focus, and purposely so'. Both 'hatred' and 'incitement' have a very high threshold, the reality is that there are likely to be relatively few circumstances where both are met.³⁰ The author witnesses 'an expectations gap' and 'a frustration gap' between community aspirations from this legislation and the reality of its limited application and implementation to date.³¹ Ryan criticised the absence of gender and gender

²⁵ Cowhey, 2006, p. 42.

²⁶ Cowhey, 2006, p. 43.; cf. Schweppe and Walsh, 2008, pp. 62–64. However, this is not unique to Ireland. For a UK perspective, see Coe, 2022, pp. 57–58. A fine line should be drawn between drafting legislation which under-/over-criminalise the hate speech.

²⁷ Schweppe and Walsh, 2008, pp. 55–56.

²⁸ Schweppe and Walsh, 2008, p. 59.

²⁹ A good example of this is the case of *DPP v O'Grady*. 'In the O'Grady case the defendant driver of a coach refused to allow a Gambian man to board at the public bus stop while the man was eating a sandwich. In doing so the driver subjected the individual to extremely derogatory remarks to the effect that he as a black man lacked the civilised standards of behaviour of the Irish white man. His conviction the District Court was overturned on appeal by the Circuit Court when it emerged that only two witnesses (apart from the Gambian man himself) had heard the offensive words and they were entirely supportive and sympathetic to the Gambian man. They were not incited to hate Gambians or non-whites as a result of the bus driver's conduct. Accordingly, an essential component of the offence had not been established and so the Circuit Court judge felt that it would be unsafe to uphold the conviction.' (Schweppe and Walsh, 2008, p. 61.)

³⁰ Taylor, 2011, p. 30.

³¹ Taylor, 2011, p. 31.

identity among the protected characteristics on which hatred is based, leaving transgender people outside the scope of its protection.³²

A 2014 report, aiming to progress the discussion of and generate an impetus for, legislative change in the area of hate crime in Ireland, has already directly concluded that 'It is clear that the Irish legal system is largely incapable of punishing hate crimes adequately'.³³ The report called for a number of reforms related to the PIHA – for example, it suggested that the the Act should create four new hostility based offences: assault aggravated by hostility; harassment aggravated by hostility; criminal damage aggravated by hostility; and public order aggravated by hostility. In addition, the authors proposed to add new elements to the law, e.g. introducing an offence of subjecting another person to threatening, abusive or insulting words about his or her personal characteristics or perceived characteristics, with the result that the person feels threatened or fearful for his safety or for that of his companions or for his property.³⁴

Haynes and Schweppe in their country report claimed that PIHA 'criminalises incitement to hatred, however it is aimed at criminalising hate speech and is thus purposefully narrow in its scope and by its nature not suited to addressing hate crime'.³⁵ Like Ryan in his above-mentioned paper, Haynes and Schweppe emphasized that PIHA is limited in terms of its protection of groups. By only naming race, colour, nationality, religion, ethnic or national origins, the Act ignores incitements to hatred against other communities, most obviously disabled people, intersex and transgender people, asylum seekers and refugees, and, arguably, the Roma community.³⁶ In their summary conclusion, they recommended the reform of the PIHA, in particular to address cyber hate and to protect a more inclusive range of groups.³⁷

1.2. Re-regulating hate crimes: the Criminal Justice (Hate Offences) Act 2024

In 2019, the Department of Justice and Equality launched a public consultation on the revision of the PIHA.³⁸ The lawmakers sought the views of experts and society on four main issues:

³² Ryan, 2013, p. 77.

³³ Schweppe et. al., 2014, p. 15.

³⁴ Schweppe et. al., 2014, pp. 46–47.

³⁵ Haynes and Schweppe, 2017, p. 11.

³⁶ Haynes and Schweppe, 2017, p. 58.

³⁷ Haynes and Schweppe, 2017, p. 203.

³⁸ Department of Justice and Equality, 2019

1. the list of protected characteristics covered by the PIHA and whether these should be changed;
2. the use of the term ‘hatred’ in the PIHA and whether this should be changed;
3. whether the wording of the PIHA is adequate to deal with online communications;
4. the need to prove the intent or likelihood of stirring up hatred and whether this should be changed.³⁹

Regarding the use of the term ‘hatred’ in the PIHA, the ministry’s paper recalls that the words or material must be intended or likely to stir up ‘hatred’ against one of the protected list of groups – and this is a high threshold.

Notable among the submissions received was a proposal from the Law Society, which made the following recommendations to the legislator:

1. The protected characteristics covered by the PIHA should be broadened to include those based on gender, disability, civil status, family status and age, whether actual or perceived.
2. The key term of ‘hatred’ should be clearly defined in line with that employed by the European Commission against Racism and Intolerance and the UN Special Rapporteur.
3. Any review or reform of the legal framework of hate speech must also address the issue of online incidents of hate speech. Where it reaches sufficiently serious levels, there should be criminal measures in place to deal with such offences.
4. The mental element in the current legislation of intention to stir up is too high a threshold. The requirement to prove the offence of incitement to hatred should be lowered to recklessness.⁴⁰

In April 2021, the Minister for Justice received approval from the Cabinet to publish the *General Scheme of the Criminal Justice (Hate Crime) Bill 2021*. The draft was later thoroughly revised and renamed to *Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022* (hereinafter IVVHO Bill) and was published on 1 November 2022.⁴¹ The IVVHO Bill aimed to

- (a) repeal the PIHA and replace it with provisions creating new incitement to violence or hatred offences;

³⁹ Department of Justice and Equality, 2019, pp. 4–6.

⁴⁰ Law Society of Ireland, 2020, p. 5.

⁴¹ Available at: <https://www.oireachtas.ie/en/bills/bill/2022/105/>

- (b) provide for an offence of condoning, denying or grossly trivialising genocide, crimes against humanity and war crimes against persons on account of their protected characteristics;
- (c) provide for offences aggravated by hatred; and
- (d) provide for a provision requiring courts to take account of evidence of hatred on the part of the perpetrator against a person or a group of persons on account of their protected characteristics or any of those characteristics during sentencing for offences other than those created under the Bill.⁴²

The Bill Digest took as a starting point that the PIHA had been deemed ineffective in combatting hate speech, in particular online hate speech – thus, ‘Ireland does not currently have any specific hate crime legislation’.⁴³

Although the Government planned to have the measures enacted by the end of 2023, some politicians of the main government party (Fianna Fáil) raised concerns about proposed new hate speech laws.⁴⁴ Finally, the IVHHO Bill was passed by Parliament in October 2024 as *the Criminal Justice (Hate Offences) Act 2024* (hereinafter HOA), following several revisions and lengthy debates. Part 2 of the IVHHO Bill (titled ‘Prohibition of Incitement to Violence or Hatred’) addressed criminalised hate speech and included several new offences, such as ‘incitement to violence or hatred against persons on account of their protected characteristics’ and ‘condonation, denial or gross trivialisation of genocide, war crimes, crimes against humanity’. However, in the absence of political consensus, and in response to concerns about freedom of expression,⁴⁵ Part 2 on hate speech (roughly one-third of the bill) was withdrawn before the law was passed.⁴⁶

The new features of the HOA can be summarised as follows.

1. As for the definition of ‘hatred’, it means hatred against a person or a group of persons in the State or elsewhere on account of their protected characteristics or any one of those characteristics.⁴⁷ This wording omits a definition of the substance of ‘hatred’.⁴⁸

⁴² Sweeney and Farmer, 2022, p. 3.

⁴³ Sweeney and Farmer, 2022, p. 16. The same applies in the UK (Coe, 2022).

⁴⁴ Bray, 2023.

⁴⁵ Some argued that the original wording of the IVHHO Bill would have risked criminalising ‘ordinary, majority-held opinions’ about sex and gender (Daly and de Brún, 2024).

⁴⁶ Law Society Gazette, 2024a.

⁴⁷ HOA, Section 2.

⁴⁸ Schweppe and Haynes, 2022, pp. 12–14. Some regards this definition as circular, and consequently the definition risks being simplified to ‘hatred is hatred’ (Daly and de Brún, 2024).

2. Concerning the ‘protected characteristic’, in relation to a person or a group of persons, means any one of the following, namely—
 - (a) race,
 - (b) colour,
 - (c) nationality,
 - (d) religion,
 - (e) national or ethnic origin,
 - (f) descent,
 - (g) gender,
 - (h) sex characteristics,
 - (i) sexual orientation, or
 - (j) disability.⁴⁹

As can be seen, the HOA maintained race, colour, nationality, religion, national or ethnic origin and sexual orientation among the protected characteristics, whereas descent, gender, sex characteristics and disability have been added to the list. In contrast to the PIHA, the HOA also outlines the meaning of some of those protected characteristics:⁵⁰

- (a) references to ‘religion’ include references to the absence of a religious conviction or belief,
- (b) references to ‘descent’ include references to persons or groups of persons who descend from persons who could be identified by certain characteristics (such as race or colour), but not necessarily all of those characteristics still exist,
- (c) references to ‘national or ethnic origin’ include references to membership of the Traveller community [within the meaning of section 2(1) of the Equal Status Act 2000],
- (d) ‘gender’ means the gender of a person or the gender which a person expresses as the person’s preferred gender or with which the person identifies and includes transgender and a gender other than those of male and female,
- (e) ‘sexual orientation’ has the same meaning as it has in section 2(1) of the Equal Status Act 2000,
- (f) references to sex characteristics shall be construed as references to the physical and biological features of a person relating to sex, and

⁴⁹ HOA, Section 3(1).

⁵⁰ HOA, Section 3(2).

(g) ‘disability’ has the same meaning as it has in section 2(1) of the Equal Status Act 2000.

3. The HOA creates new, aggravated forms of certain existing criminal offences, where those offences are motivated by prejudice against a protected characteristic (e. g. damaging property aggravated by hatred; assault aggravated by hatred; harassment aggravated by hatred).⁵¹ Where possible, these aggravated offences carry an enhanced penalty, unless the penalty is already set at the maximum possible. There is also a safeguard built into all of the offences in this Part whereby a perpetrator may be convicted of the ‘ordinary’ form of the offence if there is insufficient evidence to prove the hate element.⁵²

It should be emphasized that the PIHA remain in force, but Minister for Justice Helen McEntee noted that it needed to be updated, ‘particularly in the context of modern online communications’.⁵³

2. Fighting cyberbullying: unpacking the toolbox

In the following, we will look at the tools available in the Irish legal system to deter and sanction cyberbullying. Firstly, to illustrate the seriousness of the problem, we outline how the prevalence of bullying in the online space has evolved in the light of research conducted over the last decade. We will then discuss the relevant legislation, with a special focus on the two most important laws: the *Harassment, Harmful Communications and Related Offences Act 2020*, which entered into force in 2021, and the *Online Safety and Media Regulation Act 2022*, which was adopted at the end of 2022.

2.1. Victims and offenders in the light of researches

In Ireland, research on the prevalence of cyberbullying among young people has been published since the early 2010s.⁵⁴ One of the first such surveys found that 9% of school children aged 12-18 years surveyed admitted to

⁵¹ HOA, Sections 5–8.

⁵² Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 – Explanatory Memorandum, p. 4.

⁵³ Law Society Gazette, 2024b.

⁵⁴ For an overview, see Gaffney and Farrington, 2018.

having been involved in such bullying, while 17% reported having experienced cyberbullying.⁵⁵

Another much larger survey of more than 3,000 people (aged 12-16) found similar results: 8.6% of respondents had been actively bullied online and 13.9% had been passively bullied.⁵⁶ The data also showed that only a quarter of victims shared their stories with their parents and/or another adult, and only 1% of respondents would report an adult if they witnessed online bullying. According to the author, these latter findings strongly suggest that all current policies and prevention and intervention strategies need to promote a culture of disclosure. She claims that ‘there is an urgent need for awareness-raising programmes that not only provide students with an understanding of cyber-bullying but also provide them with the skills to intervene’.⁵⁷

Based on a questionnaire completed by 876 high school students (ages 12-16), Corcoran and her colleagues concluded that 6.3% of respondents had been victims of cyberbullying during the previous three months, while only 1.6% of students admitted to being perpetrators; in addition, an additional 1% had both perpetrated and suffered online bullying.⁵⁸ The research also showed that victims of ‘traditional’ and online bullying share similar personality and self-concept.⁵⁹

Research conducted in Ireland in 2012-13 as part of the *Health Behaviour in School-aged Children* pilot survey on a relatively small sample (318) found that 14% of 15-18 year olds surveyed were bullied in a traditional way, 10% were cyberbullied and further 10% reported that they were victims of both traditional and cyberbullying.⁶⁰ The data also showed that ‘traditional’ bullying (in the real world) and cyberbullying go together in the majority of cases, meaning that a large proportion of victims are affected by both types of bullying.⁶¹ No less worrying is the finding that victims of bullying were more likely to report poorer health and less satisfied with their lives.⁶²

Ireland had the second-highest rate of cyber-victimisation in an 11-country survey conducted in partnership with Vodafone and international polling company YouGov. In the 2015 survey, which targeted 13-18 year olds, 26% of young

55 Cotte and McGilloway, 2011. The research explored four specific forms of cyberbullying (text message, email, phone call, and picture/video clip).

56 O'Moore, 2012, p. 213.

57 O'Moore, 2012, p. 220.

58 Corcoran et al., 2012, pp. 159-160.

59 Corcoran et al., 2012, p. 160.

60 Callaghan et al., 2015, p. 201.

61 Callaghan et al., 2015, p. 202.

62 Callaghan et al., 2015, p. 201.

people in Ireland said they had experienced online bullying, while 85% said they knew someone who had been a victim of cyberbullying. The survey also found that 60% of Irish children thought that cyberbullying was worse than face-to-face bullying.⁶³

However, the phenomenon of cyberbullying has also been researched in Ireland, not only from the perspective of children, but also from the perspective of teachers and parents. A survey of Irish and Northern Irish teachers published in 2015 suggests that teachers are also aware of the problem, and expressed a desire for more guidance from their respective government departments of education. The research also found that there is uncertainty surrounding the legal responsibilities of educational institutions, and that school leaders have tended to resort to ad hoc solutions rather than the evidence-based strategies and procedures proposed by the government, and have been involved in dealing with online aggression even when it has taken place outside of school and outside-of-school hours.⁶⁴ The survey of parents also confirms a general feeling of uncertainty: they are aware of the risk posed by cyberbullying, and they are either worried or unsure about whether their children are exposed.⁶⁵

The last comprehensive research on this topic was conducted in 2019-2020.⁶⁶ The research, based on face-to-face interviews with 765 children (aged 9-17) and one parent per child (765 parents in total), focused not only on cyberbullying but also on online safety in general, and also made relevant findings on the former.⁶⁷ 11% of the children surveyed said they had experienced cyberbullying in the previous year.⁶⁸ The overall picture is improved, however, by the fact that 60% of victims said they had suffered such abuse only once or a few times. The most common method of perpetration was a text message sent to the phone (41%) or a post on social media (38%).⁶⁹ Somewhat contradicting O'Moore's 2012 research cited above, the results also showed that 67% of victims of cyberbullying turned to their parents as a source of social support.⁷⁰

63 Gaffney and Farrington, 2018, pp. 104–105.

64 Purdy and McGuckin, 2015.

65 O'Higgins Norman et al., 2016, cited in Gaffney and Farrington, 2018, p. 135.

66 National Advisory Council for Online Safety, 2021.

67 In the survey, the researchers avoided the term cyberbullying because of its complexity, and instead used a more general description of the aggressive, offensive activities that can be classified as cyberbullying National Advisory Council for Online Safety, 2021, p. 47).

68 National Advisory Council for Online Safety, 2021, p. 48.

69 National Advisory Council for Online Safety, 2021, p. 49.

70 National Advisory Council for Online Safety, 2021, p. 53.

Compared to these figures, the National Anti-Bullying Research and Resource Centre's survey during the Covid-19 closure painted a more alarming picture. The survey, which involved 504 children (aged 11-18) and 504 parents, showed that 28% of respondents had experienced online bullying during the lockdown period.⁷¹

But what is the reason for the wide variation in the surveys? Foody and her co-authors conducted a meta-analysis of 39 studies published between 1997 and 2016 that looked at bullying (including both real-life and online bullying) among Irish and/or Northern Irish children aged 4-18 years.⁷² They concluded that the measured prevalence of bullying differs mainly due to factors such as methods of data collection, the answer scales, whether the study included a definition of bullying or not, and time frame for each tool.

Of particular interest from a victimological perspective is the 2020 study that examined the post-traumatic stress induced by traditional and online bullying in five Norwegian and four Irish young people (aged 12-18).⁷³ Bullying was associated with a range of adverse effects, from persistent fear to sleep disturbance and concentration problems. The key finding of the study was that those who were bullied in both ways had more symptoms of post-traumatic stress than those who were bullied 'only' face-to-face.

2.2. The legal background

From the above surveys it is clear that online harassment has been a real problem in Ireland for a long time. In comparison, there was no specific cyberbullying law until 2021, but this did not mean that the law enforcement was completely powerless to deal with such harassment. The following laws deserve closer attention in this context:

- (a) Post Office (Amendment) Act 1951
- (b) Non-Fatal Offences Against the Person Act 1997
- (c) Children First Act 2015
- (d) Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012
- (e) Harassment, Harmful Communications and Related Offences Act, 2020
- (f) Online Safety and Media Regulation Act 2022

⁷¹ National Anti-Bullying Research and Resource Centre, 2021, p. 4.

⁷² Foody et al., 2017.

⁷³ Sjørsø et al., 2020.

Not at all in terms of its importance, but rather in terms of chronology, the first law to be mentioned is the *Post Office (Amendment) Act 1951*, which has a specific section on telephone-related offences:

13.—(1) If any person—

- (a) sends any message by telephone which is grossly offensive or of an indecent, obscene or menacing character;
- (b) sends any message by telephone which he knows to be false, for the purpose of causing annoyance, inconvenience, or needless anxiety to any other person; or
- (c) persistently makes telephone calls without reasonable cause and for any such purpose as aforesaid;

he shall be liable upon summary conviction to a fine not exceeding ten pounds, or to imprisonment for a term not exceeding one month, or to both such fine and imprisonment.

In the previous years, acts of cyberbullying were primarily punished under the harassment provisions of the *Non-Fatal Offences Against the Person Act 1997* (hereinafter NFOAPA).⁷⁴ As the Irish Government has committed to introduce new stalking and non-fatal strangulation offences as part of their zero-tolerance approach to domestic, sexual and gender-based violence,⁷⁵ the harassment-related provisions of the NFOAPA were amended in 2023. As O’Sullivan and Staunton note, ‘the new section 10(1) will modify the existing offence of harassment by simplifying the language and extending it to cover situations where the victim retrospectively becomes aware of the harassing actions’.⁷⁶ Currently the provision on harassment reads as follows:

10.—(1) A person shall be guilty of the offence of harassment where—

- (a) the person, without lawful authority or reasonable excuse, persistently, by his or her acts, intentionally or recklessly, at the time when the acts occur or when the other becomes aware of them—
 - (i) seriously interferes with another’s peace and privacy, or
 - (ii) causes alarm, distress or harm to the other,

and

- (b) the person’s acts are such that a reasonable person would realise that the acts would seriously interfere with the other’s peace and privacy or cause alarm, distress or harm to the other, at the time when the acts occurred or when the other becomes aware of them.

⁷⁴ Law Reform Commission, 2016, p. 5. (points 20–22).

⁷⁵ O’Sullivan and Staunton, 2023, p. 11.

⁷⁶ O’Sullivan and Staunton, 2023, p. 54.

The 2023 amendment of the NFOAPA introduced a new stalking offence:

- (2) A person shall be guilty of the offence of stalking where—
 - (a) the person, without lawful authority or reasonable excuse, by his or her acts, intentionally or recklessly causes another, at the time when the acts occur or when the other becomes aware of them—
 - (i) to fear that violence will be used against him or her or another person connected to him or her, or
 - (ii) serious alarm or distress that has a substantial adverse impact on his or her usual day-to-day activities,and
 - (b) the person's acts are such that a reasonable person would realise that the acts would cause the other, at the time when the acts occur or when the other becomes aware of them, to fear that violence will be used against him or her or another person connected to him or her, or serious alarm or distress that has a substantial adverse impact on his or her usual day-to-day activities.

Unlike the previous wording of the NFOAPA, the revised version gives illustrative examples of what constitutes stalking and harassing behaviour:

- (3) Without prejudice to the generality of subsections (1) and (2), the acts referred to in those subsections include the following:
 - (a) following, watching, monitoring, tracking or spying upon a person;
 - (b) pestering a person;
 - (c) impersonating a person;
 - (d) communicating with or about a person;
 - (e) purporting to act or communicate on behalf of a person;
 - (f) disclosing to other persons private information in respect of a person;
 - (g) interfering with the property (including pets) of a person;
 - (h) loitering in the vicinity of a person;
 - (i) causing, without the consent of the person, an electronic communication or information system operated by a person to function in a particular way;
 - (j) breaching a court order—
 - (i) made pursuant to this section or Part 5 of the Criminal Justice (Miscellaneous Provisions) Act 2023, or
 - (ii) otherwise restraining the person from communicating with or about the other person or, within such distance as is specified in the order, approaching the other or the place of residence, education or employment of the other person.

Section 10(4) will allow for the imposition of an order restraining the convicted person from communicating with or about or being within a specified distance of the person stalked or harassed at various venues:

- (4) Where a person is guilty of an offence under subsection (1) or (2), the court may, in addition to or as an alternative to any other penalty, order that the person shall not, for such period as the court may specify, communicate by any means with or about the other person or that the person shall not approach within such distance as the court shall specify of the place of residence, education or employment of the other person.

The *Children First Act 2015* (hereinafter CFA) regulates the obligation to report harm to children in a fairly detailed way. The CFA imposes this obligation on so-called mandated persons, which include about 30 professionals who come into contact with children by virtue of their profession, vocation or duties (such as medical practitioners, dentists, psychologists, social care workers, and teachers).⁷⁷ If a mandated person knows, believes or has reasonable grounds to suspect, on the basis of information that he or she has received, acquired or becomes aware of in the course of his or her employment or profession as such a mandated person, that a child has been harmed, is being harmed, or is at risk of being harmed, he or she shall, as soon as practicable, report that knowledge, belief or suspicion, as the case may be, to the Child and Family Agency.⁷⁸ The obligation also applies if the child reports the harm to the mandated person.⁷⁹ The CFA defines harm as assault, ill-treatment or neglect of the child in a manner that seriously affects or is likely to seriously affect the child's health, development or welfare, or sexual abuse of the child, whether caused by a single act, omission or circumstance or a series or combination of acts, omissions or circumstances, or otherwise.⁸⁰

The *Criminal Justice (Withholding of Information on Offences against Children and Vulnerable Persons) Act 2012* penalises the concealment of crimes against children (and other vulnerable groups). This makes it an offence to know that a child has been subjected to an offence defined by law (e.g. murder, rape, sexual assault) and not to disclose information that would facilitate the apprehension, prosecution or conviction of the offender to the police as soon as possible. In some instances, the bullying itself might fall into the categories of child harm that warrant disclosure to the state authorities.⁸¹

⁷⁷ CFA, Schedule 2.

⁷⁸ CFA, Section 14(1).

⁷⁹ CFA, Section 14(2).

⁸⁰ CFA, Section 2.

⁸¹ Daly, 2021.

2.3. *New act on online harassment: necessary but not sufficient?*

Since the 2010s, however, it has become increasingly clear that the NFOAPA is inadequate to curb new types of harassment in the online space that cause significant harm to victims – although there are examples of people being convicted under the Act for harassing communications on Facebook.⁸² A serious problem was that the definition of harassment as just described presupposes repeated acts of a repetitive nature (let us remember the term ‘persistently’), and the NFOAPA does not provide guidance on how many incidents are necessary to exhaust the definition.⁸³

In parallel with the proliferation of smartphones and the rise of social media, the concept of image-based sexual abuse (hereinafter IBSA) has emerged in Irish legal literature,⁸⁴ emphasising that the existing legal framework cannot effectively combat the new phenomena. In essence, IBSA refers to the taking and/or dissemination of images of private sexual content without consent.⁸⁵ According to the authors of the term, it is a broader concept than other terms used in the media (e.g. revenge porn) and can therefore be applied to a wider range of offences.⁸⁶ McGlynn and Rackley have included the following acts in the scope of the IBSA:⁸⁷

- (a) ‘Revenge porn’: a malicious ex-partner distributes private, sexual images without consent of the person(s) in the images.
- (b) Hacked or stolen images: theft and distribution of private photos of celebrities, often for financial gain.
- (c) Domestic abuse and violence: sharing – or the threat of sharing – private sexual images without consent of all the individuals involved is also used as a measure of coercion and control in abusive relationships.

82 For a description of the case, see Browne, 2019. The case: a 61-year-old man harassed an actress friend on Facebook with false and abusive comments, mainly about the victim’s qualities as a mother to her two teenage sons. The court sentenced the man to eight months’ imprisonment suspended for two years and a fine of 1,500 euros under the harassment provisions of the NFOAPA. As the report on the case points out, the prosecution for harassment under current law can be successful even when some of the evidence does not relate to a perpetrator making direct contact with an injured party.

83 Lynch, 2015.

84 McGlynn and Rackley, 2017a; McGlynn and Rackley, 2017b; McGlynn et al., 2017; Bowie, 2020.

85 McGlynn and Rackley, 2017a, p. 534.

86 McGlynn and Rackley, 2017a, pp. 535–536.

87 McGlynn and Rackley, 2017b, pp. 39–42. For a more detailed discussion of each type of offence, see McGlynn et al., 2017, pp. 29–36.

- (d) ‘Upskirting’: using a smartphone or other devices (e.g. camera hidden in the perpetrator’s shoes) to take photos under the target’s clothing (without their knowledge) and then distribute the images.
- (e) Sexualised Photoshopping: a pornographic image is superimposed onto an individual’s head/body part, such that it looks as if that individual is engaged in the pornographic activity.
- (f) Sexual extortion: the perpetrator forces the victim to take and/or share a private sexual image of themselves with the perpetrator, mainly through blackmail.
- (g) Recordings of sexual assault and rape.

The harmful effects of IBSA at the level of the individual are primarily manifested in the violation of personal and bodily integrity, human dignity and privacy, and the suppression of sexual autonomy and expression.⁸⁸ However, the negative consequences are also felt at the societal level, as the spread and possible ‘acceptance’ of IBSA carries the ‘cultural harm’ of encouraging other sexual misconduct in the longer term.⁸⁹

So, according to some, before the *Harassment, Harmful Communications and Related Offences Act 2020* (hereinafter: HHCROA) came into force, unlike most British, American and Australian jurisdictions, Irish law at present offers inadequate protection for victims of sexual cyber-harassment.⁹⁰ The above-quoted offence of harassment in the NFOAPA is not suitable to sanction a single IBSA because of the term ‘persistently’, nor is it suitable to punish non-consensual distribution of images to third parties.⁹¹

In Ireland, the draft HHCROA was published in April 2017 and revised legislation, taking into account the feedbacks of the experts, came into force in February 2021. It should be stressed that the HHCROA is specifically designed to sanction certain unlawful and harassing acts committed in the online space.

The HHCROA lists and criminalises three types of offence. The first element is related to publishing an intimate image:

2. (1) A person who distributes, publishes or threatens to distribute or publish an intimate image of another person—
 - (a) without that other person’s consent, and
 - (b) with intent to cause harm to, or being reckless as to whether or not harm is caused to, the other person,

⁸⁸ McGlynn and Rackley, 2017a, pp. 545–549.

⁸⁹ McGlynn and Rackley, 2017a, pp. 549–551.

⁹⁰ Bowie, 2020, p. 141.

⁹¹ Bowie, 2020, pp. 141–142.

is guilty of an offence.

The law also clarifies when a cause of harm can be established:

- (2) For the purposes of subsection (1), a person causes harm to another person where—
- (a) he or she, by his or her acts, intentionally or recklessly seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person, and
 - (b) his or her acts are such that a reasonable person would realise that the acts would seriously interfere with the other person's peace and privacy or cause alarm or distress to the other person.

It is noteworthy that, according to the interpretation provisions of the HHCROA, 'harm' includes also psychological harm.⁹²

To facilitate the application of the law, the HHCROA defines the term 'intimate image' in detail:

'intimate image', in relation to a person, means any visual representation (including any accompanying sound or document) made by any means including any photographic, film, video or digital representation—

- (a) of what is, or purports to be the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
- (b) of the underwear covering the person's genitals, buttocks or anal region and, in the case of a female, her breasts,
- (c) in which the person is nude, or
- (d) in which the person is engaged in sexual activity.⁹³

The second offence is recording, distributing or publishing intimate image without consent:

- 3.** (1) Subject to subsection (2), a person is guilty of an offence where—
- (a) he or she records, distributes or publishes an intimate image of another person without that other person's consent, and
 - (b) that recording, distribution or publication, as the case may be, seriously interferes with that other person's peace and privacy or causes alarm, distress or harm to that other person.

⁹² HHCROA, Section 1.

⁹³ HHCROA, Section 1.

- (2) Subsection (1) shall not apply to a person who distributes or publishes an intimate image for the purpose of the prevention, investigation or prosecution of an offence under this section.

This second element differs from the previous one in that in the first one the purpose of the offence is explicitly to cause harm the other person.

The third offence sanctioned by the HHCROA is distributing, publishing or sending threatening or grossly offensive communication:

- 4.** (1) A person who—
- (a) by any means—
 - (i) distributes or publishes any threatening or grossly offensive communication about another person, or
 - (ii) sends any threatening or grossly offensive communication to another person,
 - and
 - (b) with intent by so distributing, publishing or sending to cause harm, is guilty of an offence.
- (2) For the purposes of subsection (1), a person intends to cause harm where he or she, by his or her acts, intentionally seriously interferes with the other person's peace and privacy or causes alarm or distress to the other person.

Similar to the PIHA, body corporate may be held criminally liable under the HHCROA:

- 6.** (1) Where an offence under this Act is committed by a body corporate and the offence is proved to have been committed with the consent or connivance of, or to be attributable to any wilful neglect of, a person who, when the offence was committed, was a director, manager, secretary or other officer of the body corporate or of a person purporting to act in such a capacity, that person, as well as the body corporate, is guilty of an offence and is liable to be proceeded against and punished as if guilty of the first-mentioned offence.

The HHCROA contains an important specific provision on under-17s: where a child under 17 years of age is charged with an offence under the Act, no further proceedings in the matter (other than any remand in custody or on bail) shall be taken except by or with the consent of the Director of Public Prosecutions.⁹⁴

⁹⁴ HHCROA, Section 8.

While experts have hailed the HHCROA as a significant step forward, it has of course also been criticised. Some of the criticisms pointed out – already after the publication of the draft HHCROA – that it would be more appropriate to use the term IBSA instead of ‘harmful communication’ in the title of the law, as this term more vividly describes the acts to be sanctioned. It also follows that these offences should be recognised as sexual offences.⁹⁵ On the one hand, because the images which are the subject of the offences are sexual in nature, which is precisely why they go viral and why there is a ‘market’ for such images. On the other hand, the communications surrounding the images (comments, threats, etc.) also contain sexual content. As McGlynn and Rackley emphasize, ‘The women in the images are harassed and abused for transgressing expected norms of women’s sexuality. They are castigated for exercising sexual agency (for taking sexual images or ‘allowing’ them to be taken)’.⁹⁶ Thirdly, it must also be borne in mind that such images violate the right to sexual freedom and sexual autonomy of the victim, who is usually a woman. “The impact of image-based sexual abuse is that all women are made to feel constrained in their sexual choices and expression” – warn the authors.⁹⁷

Some of the experts also criticised the wording of the provisions of the HHCROA. As explained above, the act of recording, distributing or publishing an intimate image without consent is punishable if the recording, distributing or publishing seriously interferes with that other person’s peace and privacy or causes alarm, distress or harm. According to McGlynn and Rackley, it follows that it requires the prosecution to prove – presumably by requiring evidence from the victim-survivor – that the defendant actually interfered with a victim’s peace/privacy or caused actual harm to her/him. This is problematic in two respects. On the one hand, ‘there is a real danger this provision reifies an ‘ideal victim’ by predetermining what is seen to be the ‘appropriate’ response from victims-survivors’. The authors argue that, while many victims of harassment suffer significant harm, there are some who ‘only’ feel anger towards the perpetrator – which is not in principle sufficient to establish the facts. On the other hand, it is also more difficult to prosecute when the victim of harassment is unaware that a crime has been committed against her (e.g. because she did not realise that intimate pictures of her had been shared on social media). McGlynn and Rackley also point out that, because of the above criteria, this is a far more restrictive provision than is provided in most other (for example, Scottish or British) jurisdictions.⁹⁸

⁹⁵ McGlynn and Rackley, 2017b, pp. 42–43.

⁹⁶ McGlynn and Rackley, 2017b, p. 43.

⁹⁷ McGlynn and Rackley, 2017b, p. 43.

⁹⁸ McGlynn and Rackley, 2017b, pp. 45–46.; cf. Bowie, 2020, pp. 146–147.

‘Without consent’ as a factual element has also been criticised. The draft HHCROA initially included a definition of consent as ‘the agreement by choice of a person who has the freedom and capacity to make that choice’. This solution was criticised by Bowie on the grounds that the draft did not specify the circumstances in which consent could *not* be deemed to have been given.⁹⁹ However, this definition was removed from the final version of the HHCROA, so that concerns remained.

Bowie also drew the attention of the lawmaker to two forms of cyberbullying and sexual harassment to which, in her view, the HHCROA does not apply.¹⁰⁰ One of these is audio recordings of sexual assaults or abuse, on which the author does not elaborate, but if we assume that the definition of intimate images is based on visual representation, it is at least questionable to what extent an audio recording can be considered to be a factual matter.¹⁰¹ The other type of offence is deepfaking, where the perpetrator, usually using artificial intelligence software, manipulates the victim’s face by superimposing it on a picture or, more recently, a video of another person, thus swapping the two faces. Bowie believes that the HHCROA’s definition of an intimate image is not sufficiently inclusive to encompass deepfake forms of offending.

In addition to the previous two forms of harassment, Bowie also mentioned a third form, cyberflashing, which involves sending strangers unsolicited images of an obscene and sexual nature through online messaging platforms.¹⁰² According to the author, it is paradoxical that under the *Criminal Law (Sexual Offences) Act 2017*¹⁰³ the exposure of a person’s genitals with ‘intent to cause fear, distress or alarm to another person’ in a public place is characterized as a criminal offence (provided that the offence is intended to cause fear, distress or alarm), yet the distribution of images online featuring genitalia is not defined as such. The fact that this type of harassment is not covered by either the first or second elements of the HHCROA can be explained by the fact that these offences punish the recording, distribution, etc. of images of *another* person, but cyberflashing can also be committed with a photograph of one’s *own* genitals. It should be stressed, however, that the unsolicited sending of such images is likely to fall under the third element of the HHCROA (distributing, publishing or sending

⁹⁹ Bowie, 2020, pp. 147–148.

¹⁰⁰ Bowie, 2020, pp. 149–151.

¹⁰¹ Although the above definition of an intimate image includes the phrase ‘including accompanying sound’, if it is an exclusionary-lag sound recording, it can hardly be an intimate image.

¹⁰² Bowie, 2020, p. 151.

¹⁰³ Criminal Law (Sexual Offences) Act 2017, Section 45(1).

threatening or grossly offensive communication), as these images may also be capable of causing harm.

2.4. Safe even online? The Online Safety and Media Regulation Act 2022

As Facebook has admitted,¹⁰⁴ online communication was already covered by the existing PIHA, as it is possible to engage in abusive, insulting and hateful communication on social media. However, the PIHA is less applicable to regulating the online world, as the Irish government has recognised.¹⁰⁵ It is telling that in July 2020, a prominent lawyer publicly called on the Minister for Justice to set up a committee to review the regulatory options for social media. According to the lawyer, while the economic benefits Facebook and other tech giants had brought to Ireland cannot be ignored, ‘They nonetheless should incur a duty to protect citizens and the international community from online attacks, harassment, hate speech and fake news, which can often result in devastating consequences for the victims’.¹⁰⁶

An important step towards the proposed legislation was Online Safety and Media Regulation Bill, which was published in December 2020.¹⁰⁷ Two years later, in December 2022, the long anticipated *Online Safety and Media Regulation Act 2022* (hereinafter OSMRA) was signed into Irish law. The OSMRA aims to create a new online safety framework regime, taking into account the Audiovisual Media Services Directive (Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010) and to respond to the rise and spread of certain harmful online content. The OSMRA brings about a major overhaul of media and content regulation in Ireland by amending the *Broadcasting Act 2009*, implementing the revised Audiovisual Media Services Directive and aligning the regulation of traditional broadcasting services and audiovisual on-demand media services. As a summary of the law put it, ‘The new measures under the Act are wide-ranging, affecting not only traditional media broadcasters but also many audiovisual media services/internet service providers, including video-sharing platform services, who previously only faced limited regulatory oversight’.¹⁰⁸ It is also noteworthy, that the OSMRA brings video-sharing platform service, such as YouTube, within the scope of Irish regulation for the first time.

¹⁰⁴ Gallagher, 2020.

¹⁰⁵ Gallagher, 2020.

¹⁰⁶ The Irish News, 2020.

¹⁰⁷ For the background and presentation of the Bill, see Howlett, 2022a; Howlett, 2022b; Farmer, 2022.

¹⁰⁸ Woods et al., 2023.

The OSMRA covers all electronic and online media, including on-demand providers, video-sharing services and the so-called relevant online service, which means ‘a video-sharing platform service the provider of which is under the jurisdiction of the State, or any other information society service [...], the provider of which is under the jurisdiction of the State, and on which user-generated content is made available (directly or through providing access to another service)’.¹⁰⁹ The new regulatory framework for online safety will be overseen by an Online Safety Commissioner as part of the wider MC.

The OSMRA is reforming the media oversight system by creating a new and potentially powerful Media Commission (hereinafter MC), which will have a range of powers to promote online safety, including various investigative and sanctioning powers. The MC have the responsibility to oversee the updated regulations for broadcasting, audio-visual on-demand media services and video-sharing platform services. The Online Safety Commissioner, as part of the wider MC

An important innovation of the law is the definition of harmful online content:

- 139A.** (1) For the purposes of this Act, online content is ‘harmful online content’ if it is one of the following 2 kinds:
- (a) content that falls within one of the offence-specific categories of online content defined in subsection (2);
 - (b) content that—
 - (i) falls within one of the other categories of online content defined in subsection (3), and
 - (ii) meets the risk test defined in subsection (4).
- (2) The offence-specific categories of online content are—
- (a) the categories listed in Schedule 3,¹¹⁰ and
 - (b) any category specified for the purposes of this paragraph by order under section 139B.
- (3) The other categories of online content are:
- (a) online content by which a person bullies or humiliates another person;

¹⁰⁹ OSMRA, Section 3(1)(t).

¹¹⁰ Schedule 4 lists 42 types of harmful online content (offence-specific categories), e.g. online content by which a person

- publishes or broadcasts matter likely to lead members of the public to identify a person as the complainant in relation to a charge of a sexual assault offence
- counsels the suicide of another
- harasses another
- distributes or publishes or threatens to distribute or publish an intimate image.

- (b) online content by which a person promotes or encourages behaviour that characterises a feeding or eating disorder;
 - (c) online content by which a person promotes or encourages self-harm or suicide;
 - (d) online content by which a person makes available knowledge of methods of self-harm or suicide;
 - (e) any category specified for the purposes of this paragraph by order under section 139B.
- (4) Online content meets the risk test for the purposes of subsection (1)(b)(ii) if it gives rise to—
- (a) any risk to a person's life, or
 - (b) a risk of significant harm to a person's physical or mental health, where the harm is reasonably foreseeable.

The explanatory note of the OSMRA explicitly refers to the fact that these points include incitement to violence or hatred, as well as cyberbullying.

However, the OSMRA enables the MC to specify other harmful online content:

- 139B.** (1) If the Commission makes a proposal to the Minister that a category of online content should be specified for the purposes of section 139A(2) (b) or (3)(e), the Minister may make an order giving effect to the proposal.

As for the designation of online services, the MC may designate a relevant online service as a service to which online safety codes may be applied.¹¹¹ Concerning the online safety codes, the OSMRA stipulates the following:

- 139K.** (1) The Commission may make codes ('online safety codes'), to be applied to designated online services in accordance with section 139L.
- (2) An online safety code may make provision with a view to ensuring—
- (a) that service providers take appropriate measures to minimise the availability of harmful online content and risks arising from the availability of and exposure to such content,
 - (b) that service providers take any other measures that are appropriate to protect users of their services from harmful online content,
 - (c) that service providers take any other measures that are appropriate to provide the protections set out in Article 28b(1)(a), (b) and (c) of the Directive, and

¹¹¹ OSMRA, 139E(1).

- (d) that service providers take any measures in relation to commercial communications on their services that are appropriate to protect the interests of users of their services, and in particular the interests of children.

The complaints handling is also worth a deeper look. Under the OSMRA, the Online Safety Commissioner will be able to create a scheme for nominated bodies such as expert NGOs or charities to bring forward issues with online services to the Commissioner's attention. As O'Neill notes 'This is considered an important and innovative means of ensuring that there is a mechanism for the regulator to tap into the insights of those who work closely with children and adults impacted by harmful online content'.¹¹²

Not surprisingly, OSMRA has also been criticised by professionals. Some of the criticisms point to the overly broad definition of the range of services that would be covered by the Act. On the other hand, it was claimed that the Online Safety and Media Regulation Bill may conflict with the Digital Services Act, which is taking shape in the EU arena, raising the question of whether it would not be more appropriate for the Irish legislator to wait for the adoption of the Digital Services Act.¹¹³ In addition, a non-profit organisation dedicated to supporting the civil liberties and human rights of people has argued that the definition of harmful online content is extremely vague and could seriously infringe on freedom of expression.¹¹⁴

The OSMRA, as noted above, extends its scope even more clearly to social media platforms, which almost immediately provoked opposition from Facebook. Following the publication of the Bill, the company indicated that there should be a carve-out provision in the legislation to exempt intermediaries from liability for content posted on their platforms – otherwise intermediaries could be held liable for content over which they have no control.¹¹⁵

3. From school policies to hotlines: ways of prevention

In Ireland, the prevention and treatment of bullying in schools has been a priority since the early 1990s. Significantly, as early as 1993, the Department

¹¹² O'Neill, 2022, p. 3.

¹¹³ Kirk et al., 2022.

¹¹⁴ Slattery, 2021. The same dilemmas have arisen in relation to the UK's draft legislation on the same subject (Coe, 2022).

¹¹⁵ Slattery, 2021.

for Education published a guide to curb the phenomenon,¹¹⁶ and in 1998 an anti-bullying programme was piloted in 42 primary schools in County Donegal, involving teachers, parents and pupils, and, by definition, focusing ‘only’ on combating offline aggression.¹¹⁷ Following the researches conducted in the early 2010s – referred to above – the government’s Anti-Bullying Working Group published a comprehensive 126-page report titled *Plan On Bullying* (hereinafter: Report) in early 2013, in which, among other things

- set out some of the definitions and research around what constitutes bullying and the different types and forms of bullying behaviour,
- assessed who are the most affected groups (both perpetrators and victims),
- summarised the possible effects of harassment,
- presented the perceptions of children and young people,
- outlined the school’s responsibilities, and
- outlined what the school’s tasks are and made recommendations to reduce the bullying phenomenon.¹¹⁸

The Report, which covers both offline and online bullying, stresses that schools alone cannot solve this problem and that a complex strategy involving parents, children, the media and authorities is needed. (‘Bullying is a complex social issue and can occur in many different settings including in the home, in wider family and social groups and during sporting and youth club activities’.)¹¹⁹ It suggests that when bullying is discussed in relation to schools, it should include

- deliberate exclusion, malicious gossip and other forms of relational bullying,
- cyberbullying,
- sexual bullying and
- identity based bullying (specifically including homophobic bullying, transphobic bullying, racist bullying and bullying of those with disabilities or special educational needs).¹²⁰

The Report also pointed out that cyberbullying differs from offline forms of bullying in a number of ways. One of these is that it can be perpetrated essentially anywhere and at any time, and the home is no longer a safe haven from

¹¹⁶ Department for Education, 1993.

¹¹⁷ Farrington-Ttofi, 2009, p. 49.

¹¹⁸ Department for Education and Skills, 2013a.

¹¹⁹ Department for Education and Skills, 2013a, p. 10.

¹²⁰ Department for Education and Skills, 2013a, p. 28.

bullying. In addition, young people posting messages on the Internet do not feel as responsible for their actions as they might otherwise. A further difference is that cyberbullying against children is often hidden from parents due to the nature of online communication, and in many cases the identity of the perpetrator is not known.¹²¹

Following the Report, the Department for Education and Skills soon published the *Anti-Bullying Procedures for Primary and Post-Primary Schools* (hereinafter *Procedures*),¹²² which some consider to be the most important development in Ireland in the last 20 years in addressing the issue.¹²³ The primary aim of the *Procedures* is to provide guidance to school leaders on how to prevent bullying, how to intervene and how to deal with the harmful consequences of bullying. First and foremost, the *Procedures* require school leaders to develop an anti-bullying policy.¹²⁴ It should be stressed that the document gives a broad definition of bullying: ‘unwanted negative behaviour, verbal, psychological or physical, conducted by an individual or group against another person (or persons) and which is repeated over time’.¹²⁵ The *Procedures* explicitly states that, in line with the concept of the Report, this definition includes cyberbullying and identity-based harassment, and then provides a seven-item illustrative list of what constitutes bullying (physical aggression, intimidation, isolation/exclusion and other relational bullying, cyber-bullying, name-calling, damage to property and extortion).¹²⁶ As for cyberbullying, the *Procedures* note that it is carried out through the use of information and communication technologies and, thus, does not require face-to-face contact, and can occur at any time. The *Policies* devote a great deal of space to the development of good practice, identifying a trusting school climate and the cooperation of school management, teachers, pupils and parents as the most important factors.¹²⁷

Some three years later, a survey of 918 school principals looked at the number of reported cases of bullying in schools and the attitudes of institutions.¹²⁸ The survey found that nearly 80% of schools in the survey reported nine or fewer

121 Department for Education and Skills, 2013a, pp. 37–38.

122 Department for Education and Skills, 2013b.

123 Foody et al., 2018, p. 129.

124 Department for Education and Skills, 2013b, p. 5. It should be noted, however, that a 2013 survey already showed that all 44 schools included in the study implemented policy to counter traditional bullying and the majority (32 of 44 respondents) addressed cyberbullying within this policy (Corcoran and McGuckin, 2014).

125 Department for Education and Skills, 2013b, p. 5.

126 Department for Education and Skills, 2013b, pp. 9–10.

127 Department for Education and Skills, 2013b, pp. 21–35.

128 Foody et al., 2018. It should be noted that the researchers contacted the principals of all 4028 schools with the questionnaires, but only 23% returned (p. 130).

cyberbullying incidents per term, meanwhile, very few principals (2%) reported more than 20 bullying incidents in their school across term.¹²⁹ However, the authors were somewhat sceptical about these figures, as surveys based on interviews with pupils suggest that far more bullying occurs.¹³⁰ Notwithstanding, it is undoubtedly a positive development that no less than 99.8% of the schools surveyed reported having an anti-bullying policy present in their school, and 99% agreed with the question 'staff in my school are clear on what steps to take to tackle bullying behaviour'. A similar proportion of respondents said that

the school had procedures for the formal noting and reporting of bullying. In contrast, just over half of schools have a specific member of staff had been appointed to investigate and tackle bullying in the school.¹³¹ The research leaders stressed that further research is needed to investigate the nature and type of these policies and if indeed they are detailed enough and indicated that bullying victims should be dealt with primarily by professionals, as teachers have limited capacity to do so.¹³²

In addition to school-focused prevention efforts, awareness-raising and educational programmes are also noteworthy. These include the *Internet Safety Awareness Centre*,¹³³ which offers educational materials and advice to children, parents and teachers on how to avoid online dangers, including cyberbullying.¹³⁴ The website shows that a number of innovative initiatives have been taken in recent years to reduce online bullying and Internet awareness. Some examples of initiatives and projects include:

- (a) In 2013, a *Cyberbullying Awareness Event* was organised involving hundreds of secondary school students from County Limerick, where students acted out online bullying situations and then shared their experiences.¹³⁵
- (b) In 2014, the *CyberPsychology Research Centre* launched *Cyber Pal*, an initiative to provide advice to young children on how to deal with cyberbullying situations and to encourage safe and responsible online behaviour.¹³⁶
- (c) In 2015, a free online training material and handbook for teachers was produced to give them an idea of how to deal with cyberbullying in the school context.¹³⁷

129 Foody et al., 2018, p. 131.

130 Foody et al., 2018, p. 134.

131 Foody et al., 2018, pp. 132–133.

132 Foody et al., 2018, pp. 134–135.

133 <https://www.webwise.ie/>

134 <https://www.webwise.ie/parents/cyberbullying-a-guide-2/>

135 <https://www.webwise.ie/news/cyberbullying-awareness-event-2/>

136 <https://www.webwise.ie/teachers/new-cyber-pals-initiative-to-mark-sid2014-2/>

137 <https://www.webwise.ie/teachers/myselfie-and-the-wider-world-is-launched/>

- (d) In 2018, the *Webwise Youth Panel* was announced, inviting teenagers to share their ideas on how to reduce cyberbullying and promote a harassment-free online life at national level.¹³⁸
- (e) Also in 2018, the *Best Anti-Cyberbullying Campaign* competition was launched, open to schools and youth organisations.¹³⁹
- (f) In 2020, a comprehensive guide to help and support victims of cyberbullying was published, outlining how to support victims of online bullying.¹⁴⁰
- (g) In 2021, *Respectful Online Communication and Cyberbullying Webinar* was launched designed for post-primary teachers, exploring how to address the topic of cyberbullying and promote respectful communication.¹⁴¹

In addition to the Internet Safety Awareness Centre, it should also be noted that there is a dedicated research institute in Ireland dealing with the phenomenon of harassment. The *Anti-Bullying Centre*, based at the University of Dublin, takes a multidisciplinary approach to researching forms of bullying and online safety issues, with a number of projects, training programmes and academic publications.¹⁴²

Finally, there are also platforms for reporting various insults. The *Childline* site is specifically aimed at children and minors, and provides advice on a wide range of problematic situations, from unwanted pregnancy to cyberbullying and relationship violence.¹⁴³ Reporting can be done online or by phone. The other important platform is the *Hotline*,¹⁴⁴ a website that has been operating since 1999, where illegal online content, including abuse of intimate images, can be reported.¹⁴⁵ It should also be mentioned that the police also have a dedicated information page for dealing with cyberbullying abuse.¹⁴⁶

138 <https://www.webwise.ie/trending/join-the-webwise-youth-panel/>

139 <https://www.webwise.ie/uncategorized/best-anti-cyberbullying-campaign/>

140 <https://www.webwise.ie/news/youth/be-an-upstander-not-a-bystander/>

141 <https://www.webwise.ie/teachers/advice-teachers/respectful-online-communication-and-cyberbullying-post-primary-webwise-webinar/>

142 <https://antibullyingcentre.ie/about-us/>

143 <https://www.childline.ie/>

144 <https://www.hotline.ie/>

145 <https://www.childline.ie/>

146 <https://www.garda.ie/en/crime-prevention/online-harassment.pdf>

Summary

As this chapter has highlighted, the legal framework of both hate speech (more recently known as hate crime) and online harassment in Ireland is undergoing significant changes, with the Harassment, Harmful Communications and Related Offences Act 2020 and the Online Safety and Media Regulation Act 2022 having signed into law three years ago and one year ago, respectively. The harassment-related provisions of the Non-Fatal Offences Against the Person Act 1997 were amended in 2023 as part of the Government's zero-tolerance approach to domestic, sexual and gender-based violence. In addition, the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 is currently before Seanad Éireann. It is also clear from the above that the legislator only started discussing the legislation after several years of public consultation, allowing sufficient time for the views of various professional and civil society organisations to be heard.

As regards the reform of the regulation of hate speech, we have seen that the 1989 law has been subject to criticism from several quarters since the 2000s, pointing out that the basic elements of the Prohibition of Incitement To Hatred Act set the bar too high for proof and that some of the elements are not sufficiently precise. There have been very few convictions under the law, which critics say proves that the legislation is inadequate and outdated. The Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 reflects a new approach, as the basic offences are more inclusive (guilt can be established regardless of whether the communication that was the subject of the offence was 'effective' in inciting hatred), and the Bill creates new, aggravated forms of certain existing criminal offences, where those offences are motivated by prejudice against a protected characteristic.

In the context of cyberbullying, we have highlighted that such offences were previously sanctioned under the Non-Fatal Offences Against the Person Act, which covers harassment, but since the 2010s it has become increasingly clear that this law is inadequate to curb the new type of harassment committed in the online space, which causes significant harm to victims. The Harassment, Harmful Communications and Related Offences Act which came into force in 2021, was specifically designed to sanction certain unlawful harassment offences committed online. As indicated above, there has been a strong emphasis in Irish legal literature on the criminalisation of image-based sexual abuse. The new HHCRO is particularly innovative in that it seeks to punish the dissemination, publication or threat of dissemination or publication of intimate images by means of detailed provisions. In addition, the law provides for a specific offence of threatening or grossly offensive communication. It should be emphasised

that the wording of the latter provision implies that communication about or to another person is also punishable, thus penalising defamatory acts committed behind the victim's back. Although the HHCRO is clearly seen by experts as a step forward, it has not been without its critics.

The Online Safety and Media Regulation Act 2022 is also a milestone. The basic aim of the law is to curb harmful content online, but the Act is highly divisive and, according to some, a serious blow to freedom of expression because of its overly vague wording. Ireland became one of the first EU Member States to adopt systemic regulation of online platforms in line with the EU Digital Services Act.

As we have shown in relation to cyberbullying against children, Ireland has been a major focus for the prevention and management of bullying in schools since the early 1990s. While a number of significant achievements have been made, led by the Department for Education and with the meaningful involvement of professional bodies (such as the mandatory anti-bullying policy for all schools), recent research suggests that schools still have much to do. We have also seen a remarkable number of awareness-raising and educational programmes, projects, initiatives, etc., in addition to legal instruments, which are helping to change attitudes towards cyberbullying, thus reducing the often 'invisible' bullying activities that blight the lives of thousands of young people.

Bibliography

- Bowie, E. (2020) 'Image-Based Sexual Offences and Irish Law: Does the Harassment, Harmful Communications and Related Offences Bill 2017 Provide Adequate Legal Protection for Victims?', *Trinity Women's Review*, 4(1), pp. 140–155
- Bray, J. (2023) 'Minister for Justice to meet Fianna Fáil politicians raising concerns about new hate speech laws', *Irish Times*, 5 July 2023 [Online]. Available at: <https://www.irishtimes.com/politics/2023/07/05/minister-for-justice-to-meet-fianna-fail-politicians-raising-concerns-about-new-hate-speech-laws/>
- Browne, H. (2019) 'A Rare Conviction for Cyberbullying Shows It Can Be Done', *Dublin Inquirer*, 24 April 2019 [Online]. Available at: <https://dublininquirer.com/2019/04/24/harry-a-rare-conviction-for-cyberbullying-shows-it-can-be-done>
- Callaghan, M., Colette, K., Molcho, M. (2015) 'Exploring traditional and cyberbullying among Irish adolescents', *International Journal of Public Health*, 60(2), pp. 199–206; <https://doi.org/10.1007/s00038-014-0638-7>
- Coe, P. (2022) 'The Draft Online Safety Bill and the regulation of hate speech: have we opened Pandora's box?', *Journal of Media Law*, 14(1), pp. 50–75; <https://doi.org/10.1080/17577632.2022.2083870>
- Corcoran, L., Connolly, I., O'Moore, M. (2012) 'Cyberbullying in Irish schools: an investigation of personality and self-concept', *The Irish Journal of Psychology*, 33(4), pp. 153–165; <https://doi.org/10.1080/03033910.2012.677995>
- Corcoran, L., McGuckin, C. (2014) 'Addressing bullying problems in Irish schools and in cyberspace: a challenge for school management', *Educational Research*, 56(1), pp. 48–64; <http://dx.doi.org/10.1080/00131881.2013.874150>
- Cotter, P., McGilloway, S. (2011) 'Living in an "electronic age": Cyberbullying among Irish adolescents', *The Irish Journal of Education*, 39(1), pp. 44–56
- Cowhey, D. (2006) 'Racist Hate Speech Law in Ireland: the Need for Reform', *Cork Online Law Review*, Edition V, pp. 34–45
- Daly, C. (2021) *Cyberbullying Law Update* [Online]. Available at: <https://www.ckt.ie/news/cyberbullying-law-update-2021/>
- Daly, G., de Brún, L. (2024) 'The Great Debate', *Law Society Gazette*, 23 July 2024 [Online]. Available at: <https://www.lawsociety.ie/gazette/in-depth/2024/july/the-great-debate/>
- Department for Education (1993) *Guidelines Countering Bullying Behaviour in Primary and Post-Primary Schools* [Online]. Available at: https://ppds.pdst.ie/images/stories/Guidelines/countering_bullying_behaviour_guidelines.pdf
- Department for Education and Skills (2013a) *Plan On Bullying: Report of the Anti-Bullying Working Group to the Minister for Education and Skills* [Online].

- Available at: <https://assets.gov.ie/24758/0966ef74d92c4af3b50d64d286ce67d0.pdf>
- Department for Education and Skills (2013b) *Anti-bullying procedures for primary and post-primary schools* [Online]. Available at: <https://assets.gov.ie/24429/3b6f3db2de15ebaa1f69a0856c97c8e.pdf>
- Department of Justice (2021) *Tough sentences for hate crimes under new Bill from Minister McEntee* [Online]. Available at: <https://www.gov.ie/en/press-release/48cb5-tough-sentences-for-hate-crimes-under-new-bill-from-minister-mcentee/>
- Department of Justice and Equality (2019) *Review of the Prohibition of Incitement to Hatred Act 1989. Public Consultation*. [Online] Available at: <https://tinyurl.com/53w2y6m6>
- Farmer, I. (2002) *Insights into the OSMR Bill Part 3: Introduction to the Current Legal and Regulatory Framework* [Online]. Available at: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2022/2022-02-22_1-rs-note-insights-into-the-osmr-bill-part-3-introduction-to-the-current-legal-and-regulatory-framework_en.pdf
- Farrington, D. P., Ttofi, M. M. (2009) 'School-Based Programs to Reduce Bullying and Victimization', *Campbell Systematic Reviews*, 5(1), pp. 1–148; <https://doi.org/10.4073/csr.2009.6>
- Foody, M., Murphy, H., Downes, P., O'Higgins Norman, J. (2018) 'Anti-bullying procedures for schools in Ireland: principals' responses and perceptions', *Pastoral Care in Education*, 36(2), pp. 126–140; <https://doi.org/10.1080/02643944.2018.1453859>
- Foody, M., Samara, M., O'Higgins Norman, J. (2017) 'Bullying and cyberbullying studies in the school-aged population on the island of Ireland: A meta-analysis', *British Journal of Educational Psychology*, 87(4), pp. 535–557.; <https://doi.org/10.1111/bjep.12163>
- Gaffney, H., Farrington, D. P. (2018) 'Cyberbullying in the United Kingdom and Ireland' in Baldry, A. C., Blaya, C., Farrington, D. P. (eds.) *International Perspectives on Cyberbullying: Prevalence, Risk Factors and Interventions*, 1st edn. Cham: Palgrave Macmillan, pp. 101–143
- Gallagher, C. (2017) 'Courts Service reveals five convictions for hate crime since 1989. Current law not “fit for purpose” claim campaigners as racist incidents continue to rise', *Irish Times*, 19 June 2017 [Online]. Available at: <https://www.irishtimes.com/news/crime-and-law/courts-service-reveals-five-convictions-for-hate-crime-since-1989-1.3124352>
- Gallagher, C. (2020) *Facebook seeks exemption from Government's proposed hate speech laws. Technology companies worried about 'onerous obligations'* [Online]. Available at: <https://www.irishtimes.com/news/crime-and-law/>

facebook-seeks-exemption-from-government-s-proposed-hate-speech-laws-1.4442302

- Government of Ireland (2004) *First National Report by Ireland (United Nations International Convention on the Elimination of All Forms of Racial Discrimination) Dublin* [Online]. Available at: <https://www.justice.ie/en/JELR/1st+National+Report+Elim+of+Racism.pdf/Files/1st+National+Report+Elim+of+Racism.pdf>
- Harel, A. (2021) ‘Hate Speech’ in Stone, A., Schauer, F. (eds.) *The Oxford Handbook of Freedom of Speech*, 1st edn. Oxford: Oxford University Press, pp. 455–476
- Haynes, A., Schweppe, J. (2017) *Lifecycle of a Hate Crime: Country Report for Ireland*. Dublin: ICCL
- Howlett, E. (2002a) *Insights into the OSMR Bill. Part 1: Introduction and Background* [Online]. Available at: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2022/2022-02-22_1-rs-note-insights-into-the-osmr-bill-part-1-introduction-and-background_en.pdf
- Howlett, E. (2002b) *Insights into the OSMR Bill. Part 2: Societal context resource guide – empirical data on online usage*. [Online]. Available at: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2022/2022-02-22_1-rs-note-insights-into-the-osmr-bill-part-2-societal-context-resource-guide_en.pdf
- Irish Human Rights and Equality Commission (2022) *Submission on the General Scheme of the Criminal Justice (Hate Crime) Bill* [Online]. Available at: <https://www.ihrec.ie/app/uploads/2022/03/Submission-on-the-General-Scheme-of-the-Criminal-Justice-Hate-Crime-Bill.pdf>
- Keogh, C. (2000) ‘The Prohibition of Incitement to Hatred Act 1989 – A paper tiger?’, *Bar Review*, 6(3), pp. 178–181
- Kirk, N., Farris, E., Shankar, K. (2022) *Ireland’s Online Safety and Media Regulation Bill: Too Little, Too Soon?* [Online]. Available at: <https://digitalpolicy.ie/explainer-irelandsonline-safety-and-media-regulation-bill/>
- Law Reform Commission (2016) *Report on Harmful Communications and Digital Safety* [Online]. Available at: <https://publications.lawreform.ie/Portal/External/en-GB/RecordView/Index/37669>
- Law Society Gazette (2024a) *Hate-speech element of criminal-justice bill axed* [Online]. Available at: <https://www.lawsociety.ie/gazette/top-stories/2024/september/hate-speech-aspect-of-criminal-justice-bill-shelved/>
- Law Society Gazette (2024b) *Bill on hate crimes passes all stages* [Online]. Available at: <https://www.lawsociety.ie/gazette/top-stories/2024/october/bill-on-hate-crimes-passes-all-stages/>
- Law Society of Ireland (2020) *Submission on the Review of the Prohibition of Incitement to Hatred Act 1989* [Online]. Available at: <https://www.lawsociety.ie/>

- globalassets/documents/submissions/submission-prohibition-incitement-to-hatred-act-1989.pdf
- Lynch, C. (2015) 'Examining the existing Irish criminal legal responses to cyber-bullying', *Irish Criminal Law Journal*, 25(1), pp. 13–23
- McGlynn, C., Rackley, E. (2017a) 'Image-Based Sexual Abuse', *Oxford Journal of Legal Studies*, 37(3), pp. 534–561.; <https://doi.org/10.1093/ojls/gqw033>
- McGlynn, C., Rackley, E. (2017b) 'More than "Revenge Porn": image-based sexual abuse and the reform of Irish law', *Irish Probation Journal*, 14(1), pp. 38–51
- McGlynn, C., Rackley, E., Houghton, R. (2017) 'Beyond "Revenge Porn": The Continuum of Image Based Sexual Abuse', *Feminist Legal Studies*, 25(1), pp. 25–46; <https://doi.org/10.1007/s10691-017-9343-2>
- National Advisory Council for Online Safety (2021) *Report of a National Survey of Children, their Parents and Adults regarding Online Safety 2021* [Online]. Available at: <https://assets.gov.ie/2044409/b9ab5dbd-8fdc-4f97-abfc-a88afb2f6e6f.pdf>
- National Anti-Bullying Research and Resource Centre (2021) KiDiCoTi: Kids' Digital Lives in Covid-19 Times: A Study on Digital Practices. Safety and Wellbeing. Key findings from Ireland [Online]. Available at: https://antibullyingcentre.b-cdn.net/wp-content/uploads/2021/12/Short-report_Covid_for-media_TM_with-Author-names-1-2.pdf
- O'Higgins Norman, J., O'Moore, M., McGuire, L. (2016) *Cyberbullying in Ireland: A survey of parents internet usage and knowledge*. Dublin: National Anti-bullying Research and Resource Centre
- O'Moore, M. (2012) 'Cyber-bullying: the situation in Ireland', *Pastoral Care in Education*, 30(3), pp. 209–223.; <https://doi.org/10.1080/02643944.2012.688065>
- O'Neill, B. (2022) *Ireland's Online Safety and Media Regulation Act (CO:RE Policy Brief Series, No. 1)*. Hamburg: Leibniz-Institut für Medienforschung – CO:RE – Children Online: Research and Evidence; <https://doi.org/10.21241/ssoar.83520>
- O'Sullivan, C., Staunton, C. (2023) *Stalking and Harassment: An Investigation of Experiences in Ireland*. Cork: University College Cork [Online]. Available at: <https://www.ucc.ie/en/media/mandc/2023StalkingandHarassmentReport.pdf>
- Purdy, N., McGuckin, C. (2015) 'Cyberbullying, schools and the law: a comparative study in Northern Ireland and the Republic of Ireland', *Educational Research*, 57(4), pp. 420–436; <https://doi.org/10.1080/00131881.2015.1091203>
- Ryan, F. (2013) 'Hate speech', in O'Sullivan, O. (ed.) *Equality and Identity: Transgender and Intersex Experience in Ireland*, 1st edn. Dublin: Transgender Equality Network Ireland, pp. 76–78.; <http://dx.doi.org/10.2139/ssrn.2397731>

- Schweppe, J., Haynes, A. (2022) Review of the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 [Online]. Available at: <https://doi.org/10.34961/researchrepository-ul.21517635.v1>.
- Schweppe, J., Haynes, A., Carr, J. (2014) *A life free from fear: legislating for hate crime in Ireland: An NGO perspective*, 1st edn. Limerick: University of Limerick
- Schweppe, J., Walsh, D. (2008) *Combating Racism and Xenophobia through the Criminal Law*, 1st edn. Limerick: University of Limerick
- Sjursø, I., Fandrem, H., Roland, E. (2020) “All the Time, Every Day, 24/7”: A Qualitative Perspective on Symptoms of Post-traumatic Stress in Long-Term Cases of Traditional and Cyber Victimizations in Norway and Ireland’, *International Journal of Bullying Prevention*, 2(2), pp. 139–148.; <https://doi.org/10.1007/s42380-019-00024-8>
- Slattery, L. (2021) State going ‘too far, too fast’ with online safety legislation. Irish Council for Civil Liberties says media Bill will restrict speech not currently illegal [Online]. Available at: <https://www.irishtimes.com/business/media-and-marketing/state-going-too-far-too-fast-with-online-safety-legislation-1.4576007>
- Sweeney, C., Farmer, I. (2022) ‘L&RS Bill Digest: Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill 2022 (Bill No.105 of 2022)’, Oireachtas Library & Research Service [Online]. Available at: https://data.oireachtas.ie/ie/oireachtas/libraryResearch/2022/2022-12-15_bill-digest-criminal-justice-incitement-to-violence-or-hatred-and-hate-offences-bill-2022_en.pdf
- Taylor, S. (2011) *Responding to Racist Incidents and Racist Crimes in Ireland*. An Issues Paper for the Equality Authority. Maynooth: National University of Ireland [Online] Available at: https://www.ihrec.ie/app/uploads/download/doc/responding_to_racist_incidents_and_racist_crimes_in_ireland.doc
- The Irish News (2020) ‘Republic’s new justice minister urged to regulate Irish-based tech giants’ [Online]. Available at: <https://www.irishnews.com/news/northernirelandnews/2020/07/06/news/republic-s-new-justice-minister-urged-to-regulate-irish-based-tech-giants-1996037/>
- Woods, G., Connolly, D., McEntaggart, E. (2023) Ireland enacts its Online Safety and Media Regulation Act and appoints its first Media Commission [Online]. Available at: <https://www.dlapiper.com/en-th/insights/publications/2023/02/ireland-enacts-its-online-safety-and-media-regulation-act-and-appoints-its-first-media-commission>

XVII. HATE SPEECH AND CYBERBULLYING IN BELGIUM: CRITICAL UPDATE REQUIRED

GABRIEL STOLLSTEINER

1. ‘Censorship can never be introduced’: Belgium’s constitutional background

In Belgium, as elsewhere, the issues raised by cyberbullying and hate speech are manifold. In legal terms, they bring into play two distinct, if not opposing, principles. On the one hand, the principle of freedom of opinion and expression, which lies at the heart of our modern democracies, and from which freedom of the press also derives. On the other hand, the preservation of public order and the need to repress prohibited behaviour.

On a technical level, the emergence of new technologies, and in particular social networks, raises the question of how to adapt existing law to new practices.

First adopted in 1831, the Belgian Constitution (hereinafter: Constitution) guarantees the principle of equality before the law, as well as equality between men and women.¹ The resulting principle of non-discrimination, which is also constitutionally recognised,² applies in particular to hate speech and cyberbullying, in that it provides the basis for criminalising speech that tends to stigmatise minorities. With regard to harassment, the Constitution provides that everyone has the right to respect for his or her private and family life, subject to the conditions laid down by law.³ Generally speaking, everyone has the right

¹ Belgian Constitution, art. 10 https://www.senate.be/doc/const_fr.html

² Belgian Constitution, art. 11.

³ Belgian Constitution, art. 22.

to lead a life in keeping with human dignity, which includes a non-exhaustive list of rights, including the right to cultural and social fulfilment.⁴

Freedom of expression is mentioned in the Constitution (along with freedom of worship), which guarantees the freedom to express one's opinions in all matters.⁵ However, the same article reserves the right to punish offences committed in the exercise of this freedom. Article 25 guarantees freedom of the press and expressly excludes the establishment of censorship. This provision is of particular importance with regard to legislation on online hate speech. In a 2012 ruling, the Court of Cassation ruled that digital broadcasting was one of the processes for reproducing a text containing the punishable expression of an opinion.⁶ As a result, the digital dissemination of texts containing the punishable expression of an opinion falls within the scope of the press offence (*délit de presse*).

As we shall see below, this has an impact on the applicability of the sanctions provided for against theoretically punishable online content. Article 150 of the Constitution requires a jury to be empanelled for press offences, making the procedure tedious and costly. However, the same article excludes from this measure press offences motivated by racism and xenophobia, which makes it easier to prosecute such offences. This exception was added in 1999 to allow better application of the anti-racism law adopted previously (we will return to this subject later). The parliamentary proceedings reveal that the constitutional revision was motivated by the *de facto* impunity of press offences inspired by racism or xenophobia.⁷

To fully grasp the implications of constitutional rules on the eventual prosecution of hate speech and online harassment, it is necessary to present the general rules applicable to said offenses.

2. Hate speech and the persistence of *de facto* impunity

In this section, we will take for the first place hate speech and its prosecution in its normative context, which happens to be rather extensive, although quite fragmented as well. We will then contrast this general set of rules with the

⁴ Belgian Constitution, art. 23.

⁵ Belgian Constitution, art. 19.

⁶ Cour de cassation, 6 March 2012, P.11.1374.N.

⁷ See the introductory statement by the authors of the proposal to revise the constitution <https://www.lachambre.be/FLWB/pdf/49/1936/49K1936002.pdf>.

special rules applicable to press offences, which contributes to a considerable imbalance in the legal structure designed to criminalise hate speech.

2.1. Hate speech's splintered legal background

In Belgium, hate speech is primarily dealt with under criminal law. As seen in the previous section, the freedom to express one's opinions is a constitutionally protected principle. Freedom of expression means that speech or actions that may be perceived as offensive or hurtful are not necessarily punishable by law. However, the Constitution also provides for the possibility of punishing offences committed in the exercise of freedom of expression.

In order to distinguish between what falls within the normal exercise of freedom of expression and what falls within the scope of punishable expressions of opinion, it is necessary to delimit the scope of repressive measures relating to hate speech. To this end, Belgian legislation identifies a number of characteristics that are protected against hate speech. These characteristics are referred to as protected criteria.

The law of 10 May 2007 to combat certain forms of discrimination⁸ (anti-discrimination law) lists a number of these protected criteria:

- (a) age, sexual orientation, marital status, birth, wealth;
- (b) religious or philosophical beliefs, political convictions or trade union membership;
- (c) the language;
- (d) state of health, disability, physical or genetic characteristic;
- (e) origin or social condition.

In addition, the law of 30 July 1981 to suppress certain acts inspired by racism or xenophobia⁹ (the antiracism law) lists the following criteria:

- (a) nationality;
- (b) a so-called race;
- (c) skin color;
- (d) descent or national or ethnic origin.

⁸ Loi du 10 mai 2007 tendant à lutter contre certaines formes de discrimination, art. 4 (hereinafter: Loi anti-discrimination) <http://www.ejustice.just.fgov.be/eli/loi/2007/05/10/2007002099/justel>

⁹ Loi du 30 juillet 1981 tendant à réprimer certains actes inspirés par le racisme ou la xénophobie Art. 4 (hereinafter: Loi antiracisme) <https://www.ejustice.just.fgov.be/eli/loi/1981/07/30/1981001359/justel>

Finally, the law of 10 May 2007 to combat discrimination between women and men¹⁰ (gender law) defines several complementary criteria:

- (a) gender (real or perceived);
- (b) pregnancy, medically assisted reproduction, childbirth, breastfeeding, maternity, family responsibilities;
- (c) gender identity, gender expression, sexual characteristics and medical or social transition.

These protected criteria may be real or supposed, granted on their own or by association, taken alone or in combination with one or more other protected criteria contained in one or other of the aforementioned laws.

Discrimination and incitement to discrimination are intentional offences. For there to be discrimination, there must be an intention on the part of the perpetrator to treat the victim unfavourably on the basis of one of the protected criteria; the perpetrator must act knowingly and voluntarily.¹¹ Therefore, to be punishable, hate speech must target a person or group corresponding to one of the protected criteria, and the expression must also include an incitement component. In each of the three laws cited,¹² the following behaviours are punishable:

- a) incitement to hatred or violence against a person or group meeting at least one of the protected criteria;
- b) incitement to discriminate against a person or group, or incitement to segregate a group covered by a protected criterion.

The anti-racism law also introduced three specific offences designed to punish certain types of behaviour: Holocaust denial, racial supremacism and membership of a group advocating discrimination or segregation.

Holocaust denial is defined in the law¹³ as the act of denying, grossly minimising, seeking to justify or approving facts corresponding to a crime of genocide, a crime against humanity or a war crime, established as such by a final decision handed down by an international court. In so doing, the offender knew or ought to have known that such conduct would likely expose a person, a group, a community or their members to discrimination, hatred or violence on the

10 Loi du 10 mai 2007 tendant à lutter contre la discrimination entre les femmes et les hommes, art. 4 (hereinafter: Loi genre) <https://www.ejustice.just.fgov.be/eli/loi/2007/05/10/2007002098/justel>

11 Mouffe, 2014, p. 153.

12 Loi anti-discrimination, art. 22; Loi antiracisme, art. 20; Loi genre, art. 27.

13 Loi antiracisme, art. 20, 5°.

basis of one of the protected grounds. Belgium refuses to see this offense as a political one¹⁴. This is far from insignificant, as political offences benefit from constitutional provisions similar to those for press offences, which would make it difficult to effectively condemn such actions.

As early as 1995, a law on Holocaust denial¹⁵ made it an offence to deny, grossly minimise, seek to justify or publicly approve of the genocide committed by the German National Socialist regime during the Second World War.

Conviction for Holocaust denial carries additional penalties. It should be noted that, in accordance with the provisions of the Criminal Code,¹⁶ the law provides that the convicted person may be deprived of certain rights:

- (a) holding public office, employment or office;
- (b) eligibility;
- (c) wearing a decoration or a title of nobility;
- (d) be a juror, expert, instrumental witness or certifier in acts;
- (e) give evidence in court other than to provide information;
- (f) manufacture, modify, repair, transfer, hold, carry, transport, import, export or transit a weapon or ammunition, or serve in the armed forces.

For the offence of Holocaust denial, this additional disqualifying penalty is imposed for a period of between 5 and 10 years.¹⁷ Indeed the court may order that the judgment be published, in full or in part, in one or more newspapers, and that it be posted, at the expense of the convicted person.

The dissemination of ideas based on racial superiority or hatred is also punishable.¹⁸ The broadcaster must have the actual intention of stirring up hatred against a specific group.

In addition, membership of or collaboration with a group or association that repeatedly advocates discrimination or segregation is punishable.¹⁹ The law therefore covers two types of situations: on the one hand, intentional membership of an association or group which, in public and on several occasions, advocates discrimination or segregation according to one of the protected

¹⁴ Lambert, 2020.

¹⁵ Loi du 23 mars 1995 tendant à réprimer la négation, la minimisation, la justification ou l'approbation du génocide commis par le régime national-socialiste allemand pendant la seconde guerre mondiale <https://www.ejustice.just.fgov.be/eli/loi/1995/03/23/1995009273/justel>

¹⁶ Code pénal, art. 31.

¹⁷ Code pénal, art. 33.

¹⁸ Loi antiracisme, art. 21.

¹⁹ Loi antiracisme, art. 22.

criteria. On the other hand, intentional collaboration with such an association or group.

For each of these types of incitement, as well as for those provided for in the anti-racism law, the expression must be public. The legislation refers to the Belgian Criminal Code (hereinafter: Code pénal)²⁰ to establish the public nature of the act in question. The act must have been carried out in one of the following circumstances:

- (a) In meetings or public places;
- (b) In the presence of several individuals, in a place that is not public, but open to a certain number of people who have the right to assemble there or frequent it;
- (c) In any place, in the presence of the offended party and before witnesses;
- (d) By printed or unprinted matter, images or emblems displayed, distributed or sold, offered for sale or exposed to public view;
- (e) By writings not made public, but addressed or communicated to several people.

The penalties are identical for all the offences mentioned above, i.e. imprisonment for between one month and one year and a fine of between fifty and one thousand euros.

Other more general offences may occasionally apply in the specific case of hate speech. These include written insults and harassment. In these cases, the discriminatory motive may constitute an aggravating factor.²¹ In Belgium, it is a punishable offence to insult someone in public by means of actions, writings, images or emblems.²² Oral insults against ordinary citizens therefore do not come under this heading. The right to lodge a complaint is reserved solely for the person who has been personally insulted.

There is therefore no single norm that covers all cases of hate speech that are punishable. This normative fragmentation has been identified as a factor complicating anti-discrimination legislation.²³ Each of the offences mentioned above is likely to fall within the definition of press offences. These are cases where a punishable expression takes the form of writing and is published using a reproduction process. The Belgian Constitution prescribes the establishment

²⁰ Code pénal, art. 444. <https://www.ejustice.just.fgov.be/eli/loi/1867/06/08/1867060850/justel>

²¹ Code pénal, art. 78 https://www.ejustice.just.fgov.be/img_1/pdf/1867/06/08/1867060850_F.pdf

²² Code pénal, art. 448.

²³ Commission d'évaluation des lois fédérales tendant à lutter contre la discrimination, 2022.

of a jury and therefore the convening of an assize (Cour d'Assise) court for press offences.

2.2 Press offense and its impact on hate speech laws' enforceability

Press offences merit a closer look because it lies at the heart of the difficulties currently encountered in the effective enforcing of criminal law in relation to incitement to hatred and related offences. To understand what justifies such a protective regime, it is useful to recall the context in which the Belgian Constitution was adopted, in 1831. The Declaration of Belgian Independence, by which the country seceded from the United Kingdom of the Netherlands in 1830, followed the Belgian Revolution in the same year. Despite the imposed and unequal nature of the union with the Netherlands, there was a degree of press freedom; however, several liberal journalists were imprisoned and exiled in 1830 for their opinions (Potter, Tielemans, Bartels, etc.). As many of them took part in the revolution only a few months later, it is hardly surprising to find that the Constitution, less than a year after the event, gave particularly wide-ranging protection to press freedom. Most of the Constituents had been revolutionaries in 1830 and they wanted to prevent a return to the attacks on the press and partisan prosecutions that had marked the Dutch regime.²⁴ By entrusting the punishment of press offences to a jury, the Constituents intended to rely on popular opinion to judge this matter. The aim was to put an end to infringements of press freedom and prevent politically motivated prosecutions.

As the Constitution provides that the press is free and that censorship cannot be established,²⁵ it is guaranteed that no action can be taken preventively: only a posteriori repression of abuses committed in the exercise of freedom of the press is possible. Finally, the principle of cascading liability (*responsabilité en cascade*) applies, whereby the liability of the author is first sought, if he or she is known and domiciled in Belgium, before that of the publisher, printer or distributor.

Hence press offences, along with political offences, constitute a separate category of offence, outside the ordinary law.²⁶ Under Belgian law, freedom of the press is subject to two limitations. The civil aspect consists mainly of the 'right of reply' (*droit de réponse*) procedure, the aim of which is to repair the damage caused to the individual. The courts' practice of imposing penalties

²⁴ Van De Kerchove et al., 2014.

²⁵ Belgian Constitution, art. 25.

²⁶ Van De Kerchove et al., 2014.

of only a symbolic one euro limits the practical scope of the civil procedure.²⁷ The right of reply is open to any natural or legal person named or implicitly referred to in a periodical.²⁸ The criminal aspect is designed to punish offences committed in the exercise of this freedom. In this respect, the privilege of jurisdiction reserved for press offences constitutes what can best be described as a special regime: it is highly unusual and significant that the Belgian Code pénal contains no provision relating to press offences. The relevant articles of the Constitution are supplemented by two contemporary texts of a regulatory nature: the decree of 19 July 1831, which re-establishes the jury,²⁹ and the decree of 20 July 1831 on the press.³⁰ Article 8 of the first decree stipulated, for example, that preventive detention could never be used for simple press offences.

One can certainly welcome the laudable intention of the authors of the Belgian Constitution of 1831 to guarantee such a fundamental democratic principle as freedom of the press. However, when we look at the scope of application and the regime applicable to press offences, we see that the legal framework is ill-suited to contemporary issues.³¹ The Court of Cassation's interpretation is both restrictive and extensive. Restrictive, because the press offence regime applies only to written material, excluding in principle all audiovisual media. Extensive, because individual writings that undoubtedly fall into the category of insult or slander benefit from the protection in principle reserved for journalists.

We therefore find ourselves today in the paradoxical situation where press offences cover activities that are clearly not journalistic in nature, while activities that are eminently journalistic are not concerned. Admittedly, the task of disentangling where journalism ends and incitement to hatred begins is by no means easy, and it is understandable that a judge is not necessarily the best person to do this. The Court of Cassation's rigorous interpretation, which often runs counter to the more pragmatic decisions of courts of first or second instance, is often seen by legal scholars as an appeal to the legislator or even the constituent. The latter will be all the more encouraged to reform the law if it leads to solutions

²⁷ Ibid.

²⁸ Loi du 23 juin 1961 relative au droit de réponse, art. 1 <https://www.ejustice.just.fgov.be/eli/loi/1961/06/23/1961062307/justel>

²⁹ Décret du 19 juillet 1831 qui rétablit le jury.

³⁰ Décret du 20 juillet 1831 sur la presse.

³¹ Rosoux, 2005.

that are manifestly contrary to common sense.³² Worse still, for reasons of cost and the complexity of the procedure, in particular the convening of a Cour d'Assises, in practice press offences almost never result in an actual trial: there have only been three cases since the end of the Second World War. By the end of the 1990s, the problem had become so acute that the Constitution was amended to allow cases of press offences motivated by racism and xenophobia to be tried under ordinary procedure. Without this amendment, the 1981 anti-racism law would have remained, in part, a dead letter. Until the 1999 constitutional revision, only one case had resulted in a conviction for a press offence, concerning provocation to commit racist acts.³³ However, this partial solution in turn poses a problem of breach of equality, since the victims of incitement to hatred or discrimination on any other grounds are, in practice, deprived of any means of redress to have the abuse punished. Such a discrepancy between an applicant's prospects of winning his or her case owing to the motive of hatred can hardly be seen as anything other than a clear breach of the principle of equality.

In addition, and to address more directly the central issues of this work, it is essential to note that writings published on the Internet are also covered by the provisions relating to press offences. Initially, this view was based on a concern for consistency. It was unthinkable that a printed publication of a newspaper should be protected but that the same writings, published online, should not. In 2012, the Court of Cassation therefore accepted that digital distribution constituted a process similar to printing.³⁴ Since then, the Cour de cassation has defined a press offence as the infringement of the rights of either society or a citizen, through the expression of a criminal thought or opinion in printed or digital (emphasis added) material that has been distributed to the public.³⁵ However, and contrary to the interpretation of the Liège Court of Appeal,³⁶ the Court of Cassation does not make the jury's jurisdiction dependent on the relevance or social importance of the published thought or opinion, or on the more or less argued or developed nature of the offending writing, or on the notoriety

32 Cour de cassation, 7 October 2020, P.19.0644.F The defendant, the owner of a shopping centre, was prosecuted for having posted a message on the social network accusing his local councillor of corruption, along with personal insults, including about her appearance. Contrary to the Court of Appeal, the Court of Cassation concluded that mere insults could be considered as press offences.

33 A ruling by the Cour d'Assises de Hainaut on 23 June 1994 sentenced the defendants to the maximum penalties provided for by the law of 30 July 1981 designed to punish certain acts inspired by racism or xenophobia.

34 Cour de cassation, 6 March 2012, P.11.1374.N.

35 Cour de cassation, 7 October 2020, P.19.0644.F.

36 Cour d'appel de Liège, (18e ch.), 28 May 2019.

of its author. In other words, mere insults posted on social networks may not be excluded from the protection inherent to press offences.

The results of such an interpretation are predictable: in this age of ubiquitous social networking, a hate message published on an individual's profile page is treated with the same ceremonious respect as an editorial published in a daily newspaper. This has led to a proliferation of online hate speech.³⁷ Granted, in a case from 2021, a person was convicted by the Cour d'Assises de Liège of press offences and verbal threats committed in the course of his social networking activities.³⁸ The outcome of this case might lead us to believe that the current Belgian legal system is capable of responding to the phenomenon of online hate speech³⁹. But that would be forgetting that the prospect of convening a jury for every online hate publication is simply not feasible.

The institutional players involved in preventing discrimination regularly call for constitutional reform to ensure that anti-discrimination measures are consistent and that punishable acts are effectively prosecuted. For example, in 2015,⁴⁰ 2018,⁴¹ 2021⁴² and 2024,⁴³ Unia called for a revision of article 150 of the Constitution, which establishes the jury for press offences. In the last recommendation, in the form of an open letter co-signed by 39 other anti-discrimination organisations, it was noted that the current regulations were inadequate to deal with current issues, particularly with regard to social networks.

Two proposals saw the light of day in 2021, but were unable to be adopted due to the lack of the qualified two-thirds majority required for a constitutional revision. One was to extend the existing exception for press offences motivated by racist motives to any discriminatory motive.⁴⁴ The second set out in detail all the discriminatory grounds justifying an exception to the jury principle, but

37 Hugon, 2022, p. 71.

38 Cour d'assises de Liège, 13 October 2021.

39 Carneroli, 2021.

40 Freedom of the press and incitement to hatred: a parliamentary debate on Article 150 of the Constitution <https://www.unia.be/fr/legislation-et-recommandations/recommandations-dunia/liberte-de-presse-et-incitation-a-la-haine-pour-un-debat-parlementaire-sur-larticle-150-de-la-constitution>

41 <https://www.unia.be/fr/legislation-et-recommandations/recommandations-dunia/revision-des-articles-de-la-constitution>

42 "Prosecuting hate speech is simply logical" <https://www.unia.be/fr/articles/poursuivre-les-discours-de-haine-cest-tout-simplement-logique>

43 "Let's put an end to double discrimination in our Constitution" <https://www.unia.be/fr/articles/mettons-fin-double-discrimination-dans-constitution>

44 Milecan, 2021.

also proposed, by amending article 25 of the Constitution, to extend protection of the press to all written and audiovisual media.⁴⁵

In a revision of the Constitution the stakes are particularly high, not only for the victims of hate speech, but also for the journalistic profession, for whom the prospect represents both an opportunity and a risk. An opportunity, because the distinction between the written press and other media, not provided for in the Constitution but established by case law, could be eliminated. A risk, because a reduction in protection for the press in order to combat impunity for cyberbullying could have a knockback effect on the written press, which has until now benefited from this particularly broad protection. As for the prospect of making a distinction between professional journalists, who are subject to a code of ethics, and average Internet users, in order to better protect the former, this in turn raises a series of problems, particularly in terms of legal classification. In recent years, with the rise of so-called citizen media, the dividing line between professionals and ordinary citizens has become much blurred.⁴⁶

In the absence of a solution that would allow the exceptions relating to press offences to be extended, another option being considered is to change the way the justice system works. The idea would be to maintain the jury system but to make it more effective. The idea would not be to increase the number of exceptions to press offences, but rather to strengthen and modernise the jury system, since its intervention is a fundamental democratic guarantee that dates back to 1830 but is arguably still fully justified in the 21st century.⁴⁷ It should be noted, however, that this last solution, in itself, would resolve neither the incomprehensible gap in equality that currently exists between written and audiovisual content, nor the no less puzzling legal discrepancy between racist or xenophobic motives and other discriminatory motives.

This section shows that Belgium has a fairly well-developed legislative system for combating hate speech. However, the effectiveness of this legislation is seriously undermined by the combination of constitutional provisions that are ill-adapted to technological developments and a certain rigour in the interpretation of these provisions by the courts. In practice, written hate speech enjoys almost total impunity, except where it is motivated by racism or xenophobia. In the latter case, as well as in the case of hate speech conveyed in an audiovisual medium, the ordinary law procedure applies.

⁴⁵ Milecan, 2021.

⁴⁶ Milecan, 2021.

⁴⁷ Vrielink, 2022.

2.3. *Harassment, cyberbullying and related offenses*

The offence of harassment is defined in article 442bis of the Code pénal, introduced by a law of 30 October 1998.⁴⁸ The article states that anyone who harasses a person while knowing or ought to have known that this behaviour would seriously affect the peace and quiet of the person concerned will be punished by imprisonment of between fifteen days and two years and a fine of between fifty and three hundred euros, or by one of these penalties only.

The Criminal Code provides for a number of aggravating circumstances which justify doubling the minimum penalty:

- (a) Acts of harassment are committed to the detriment of a person whose situation of vulnerability due to age, pregnancy, illness, infirmity or physical or mental deficiency was apparent or known to the perpetrator.⁴⁹
- (b) One of the perpetrator's motives is hatred, contempt or hostility towards a person because of one of the protected criteria listed in section 2 on hate speech.⁵⁰
- (c) One of the perpetrator's motives is a link (real or supposed) between the victim and a person in respect of whom the perpetrator harbours hatred, contempt or hostility for one or more of the characteristics (real or supposed) listed above.⁵¹

This legal definition therefore criminalises harassment in the broad sense. There was some discussion for a time as to whether the absence of a more precise definition in the law of the concept of harassment infringed the principle of legality in criminal matters.⁵² These discussions were definitively settled following the pronouncement of several rulings by the Court of Arbitration, now the Constitutional Court, which settled the question by giving a negative answer.⁵³

Another more specific offence is provided for in article 145. § 3bis of the law of 13 June 2005 on electronic communications: it punishes by a fine of between fifty and three hundred euros and imprisonment for between fifteen days and two years any person who uses an electronic communications network or service or other means of electronic communications in order to annoy a correspondent

48 Code pénal, art. 442bis, para. 1.

49 Code pénal, art. 442bis, para. 2.

50 Code pénal, art. 442ter, para. 1.

51 Code pénal, art. 442ter, para. 2.

52 Thevissen et al., 2022.

53 Cour d'Arbitrage, 10 May 2006, n° 71/2006; Cour d'Arbitrage, 14 June 2006, n° 98/2006; Cour Constitutionnelle, 5 May 2009, n° 76/2009.

or cause damage.⁵⁴ The restrictive wording of this offence means that it does not necessarily cover all acts of cyberbullying. The text of the law does not include the term “harassment”, however the fact of using a means of telecommunication in order to annoy a correspondent or cause damage is a concept close enough to harassment. The law is specific in that it requires the perpetrator of harassment to use technological means as one of the material conditions for the offence to be defined. The definition of these technological means is contained in article 2 of the 2005 law.

The electronic communications network is defined as the transmission systems, whether or not based on a permanent infrastructure or centralised management capability and, where applicable, switching or routing equipment and other resources, including network elements that are not active, which permit the conveyance of signals by wire, by radio, by optical or by other electromagnetic means, including satellite networks, fixed (circuit- and packet-switched, including Internet) and mobile networks, systems using the electricity grid.⁵⁵

An electronic communications service is the service normally provided for remuneration via electronic communications networks and includes the following types of service:

- (a) an Internet access service;
- (b) an interpersonal communications service (e.g. messaging service);
- (c) services consisting wholly or mainly of the transmission of signals, such as transmission services used for the provision of machine-to-machine services.

In practice, this provision is aimed primarily at ‘telephone harassment’, but its scope is not limited to this: other forms of harassment committed using electronic communications are also likely to be covered. Examples include the unsolicited sending of SMS messages or emails (spamming), or the deliberate sending of computer viruses with the aim of causing damage.⁵⁶

It follows from the above that cyberbullying, insofar as it refers to harassment committed on the Internet, is not as such criminalised by a specific offence in the Criminal Code. It can take a multitude of forms, such as the creation of false profiles, the sending of harassing messages, the posting and dissemination of insulting remarks, but also compromising photos or videos, which aim to harm a person or exclude him or her from a group.⁵⁷

⁵⁴ Loi du 13 juin 2005 relative aux communications électroniques, art. 145.

⁵⁵ Loi du 13 juin 2005 relative aux communications électroniques, art. 2, 3.

⁵⁶ Leroux, 2016.

⁵⁷ Colette-Basecqz, 2018.

When harassment is committed as part of a group, the offence of participation can be applied both to harassment under the provisions of the Criminal Code and to the offence contained in the 2005 law on electronic communications. Thus, co-perpetrators and accomplices to harassment may be prosecuted in the same way as the principal perpetrator.

Under the Criminal Code, the following are considered to be co-perpetrators of a felony or misdemeanour:

- (a) Those who carry out the order or cooperate directly in its execution;
- (b) Those who, by any act whatsoever, have given such assistance to the execution of the offence that, without their assistance, the crime or misdemeanour could not have been committed;
- (c) Those who, by means of gifts, promises, threats, abuse of authority or power, machinations or culpable artifices, have directly provoked this crime or offence;
- (d) Those who, either by speeches made at meetings or in public places, or by writings, printed matter, images or emblems of any kind whatsoever, which are displayed, distributed or sold, offered for sale or exposed to public view, directly incite others to commit a crime, without prejudice to the penalties laid down by law for those who incite others to commit crimes or offences, even if these incitements are not followed up.⁵⁸

The following shall be punished as accomplices to a felony or misdemeanour:

- (a) Those who have given instructions to commit it;
- (b) Anyone who procures weapons, instruments or any other means used in the commission of a crime or misdemeanour, knowing that they were intended for that purpose;
- (c) Those who knowingly aid or assist the perpetrator or perpetrators of the crime or misdemeanour in the acts which prepared or facilitated it, or in those which consummated it.⁵⁹

The difference between a co-perpetrator and an accomplice is that the assistance is indispensable (in the first case) and accessory (in the second) to the commission of the offence. An accomplice is punished less severely than a co-perpetrator.

According to Colette-Basiecz, the act of 'liking' a publication containing disparaging remarks might be considered as participation, within the meaning of

⁵⁸ Code pénal, art. 66.

⁵⁹ Code pénal, art. 67.

the Criminal Code, if the intention to promote or encourage harassment were established. The context surrounding the facts would undoubtedly be enlightening, particularly the content of the publication and the author of the ‘like’. Intentionality is decisive, as serious carelessness is not enough to constitute guilty intent.⁶⁰

The question arose as to whether acts of cyber-harassment could be considered press offences, falling within the jurisdiction of the assize court. In a ruling dated 29 October 2013,⁶¹ the Court of Cassation accepted firstly, that the broadcasting of a video on the Internet could not constitute a press offence in the case of an audiovisual work, and secondly, that the mere fact of broadcasting a single video on the Internet could constitute the repetition inherent in the offence of harassment, given the permanent and repeated effects that such broadcasting may entail through successive consultations by the Internet users.

3. Preventing hate speech and (cyber)bullying: organisations and public policies

3.1. From prevention to reparation: the role of public organisations

In Belgium, three bodies are responsible for duties related to the three laws mentioned above, aimed at combating racism and discrimination and promoting equality between women and men. These are Unia, the Federal Institute for Human Rights (Institut fédéral des droits humains – IFDH) and the Institute for the Equality of Women and Men (Institut pour l’égalité des femmes et des hommes).

Unia is an independent public institution that fights discrimination and defends equality in Belgium. Founded in 1993 under the name “Centre for Equal Opportunities and Opposition to Racism”,⁶² its objective is to defend the equal and inclusive participation of all in all sectors of society and to ensure respect for human rights in Belgium. Its mission is set out in the cooperation agreement

⁶⁰ Colette-Basecqz, 2018.

⁶¹ Cour de cassation, (2nd Ch.), 29 October 2013.

⁶² Loi adaptant la loi du 15 février 1993 créant un Centre pour l’égalité des chances et la lutte contre le racisme en vue de le transformer en un Centre fédéral pour l’analyse des flux migratoires, la protection des droits fondamentaux des étrangers et la lutte contre la traite des êtres humains <https://www.unia.be/files/Documenten/Documenten/Wetgeving/20130817.pdf>

between the Federal State, the Regions and the Communities. It is also designated as the independent mechanism responsible for promoting, protecting and monitoring the application of the UN Convention on the Rights of Persons with Disabilities. Its task is to defend human rights in all its missions, but also to contribute to the evaluation of Belgium in terms of respect for human rights.

As a national human rights institute, Unia defends equality and fights discrimination on the basis of protected discrimination criteria, including skin colour, national or ethnic origin, philosophical or religious beliefs, disability, age and sexual orientation. Its territorial jurisdiction extends to the whole of Belgium: Unia is an inter-federal institution. This means that it operates at federal, regional and community level.

The organisation provides individual support and guidance to people who feel discriminated against, and listens to those who witness discrimination. This includes providing a reporting form and a telephone number that can be called free of charge. The idea is to give people easy, free access to personalised help, explaining their rights and seeking a solution through negotiation or, in some cases, legal action. Unia offers training for companies and institutions wishing to set up a diversity policy, and has also created an online training course on anti-discrimination legislation. Finally, it issues advice and recommendations to organisations and authorities. As a centre of knowledge and expertise, it produces publications and statistics to inform the authorities and various bodies about discrimination and diversity.⁶³

One of the most relevant aspects of Unia's work in the fight against hate speech is the search for alternatives to prosecution by offering mediation. In many situations, particularly where hate speech posted on social networks is concerned, a pedagogical approach may be better suited to helping both the perpetrator and the victim to repair the damage caused. The aim is to open a dialogue and encourage the perpetrator to understand what is at stake and to sincerely repent of his actions.⁶⁴ For example, in 2014, a student who made antisemitic statements on a social network agreed to take a training course designed to help him deal with the consequences suffered by victims of hate speech. He also agreed to visit a museum dealing with the Holocaust in Belgium and the timeless mechanisms of group pressure and collective violence, after which he spontaneously wrote a letter of apology showing how far he had come. In return for complying with the mediation agreement, the criminal

63 <https://www.unia.be/fr/a-propos-dunia>

64 <https://www.unia.be/fr/jurisprudence-alternatives/mesures-alternatives>

proceedings against him were dropped.⁶⁵ In 2020, mediation also took place in relation to a homophobic video posted on a video-sharing website.⁶⁶

We find this approach particularly interesting, as it allows a compromise solution to be found that is satisfactory to both parties: a middle ground of sorts, between impunity and the initiation of legal proceedings, especially when the perpetrators are motivated more by ignorance than by genuine malice. Rather than aiming to moralise social life by punishing individuals who have committed an offence against a criminal law, at the end of a judicial process entirely in the hands of the judge, penal mediation gives us a glimpse of the possibility of a consensual resolution of conflicts.⁶⁷

The Federal Institute for Human Rights (IFDH) was created by the law of 12 May 2019⁶⁸ in order to provide Belgium with a National Institute for Human Rights (INDH) responsible for ensuring that international human rights standards are respected and applied. The Institute's mandate extends to all issues relating to fundamental rights that fall within federal jurisdiction, except those dealt with by sectoral bodies for the promotion and protection of human rights. The Institute's mandate covers acts and omissions by public authorities, private bodies and individuals. However, its jurisdiction is solely federal, which means that it has no jurisdiction over matters decided by the communities and regions. Its scope of action is therefore still somewhat limited, as there are currently no plans to give it the power to deal with individual complaints. Its role is therefore limited mainly to issuing opinions and recommendations, and publishing reports.

The third institution that should bear mentioning is the Institute for the Equality of Women and Men. Created by the law of 16 December 2002,⁶⁹ the Institute for the Equality of Women and Men has the task of supporting gender equality policy at Belgian federal level. The law defines its objectives as follows:⁷⁰

- (a) ensure that equality between men and women is respected;

65 <https://www.unia.be/fr/jurisprudence-alternatives/mesures-alternatives/des-commentaires-antisemitismes-sur-facebook-a-la-convention-de-mediation>

66 <https://www.unia.be/fr/jurisprudence-alternatives/mesures-alternatives/un-film-homophobe-sur-youtube-conduit-a-une-mediation>

67 Mincke, 2010.

68 Loi du 12 mai 2019 portant création d'un Institut fédéral pour la protection et la promotion des droits humains

69 Loi du 16 décembre 2002 portant création de l'Institut pour l'égalité des femmes et des hommes https://www.ejustice.just.fgov.be/cgi_loi/change_lg.pl?language=fr&la=F&cn=2002121635&table_name=loi

70 Loi du 16 décembre 2002, art. 3.

- (b) combat all forms of discrimination and inequality based on a criterion protected by the law of 10 May 2007 designed to combat discrimination between women and men
- (c) develop instruments and strategies based on a gender mainstreaming approach.

In carrying out its mission, the Institute engages in dialogue and collaborates with associations, institutions, bodies and services whose activities fall, exclusively or in part, within the same field or which are immediately associated with the accomplishment of the said mission.

The law empowers the Institute to carry out the following tasks:⁷¹

- (a) to carry out, develop, support and coordinate studies and research into gender issues and equality between women and men, and to assess the gender impact of the policies, programmes and measures implemented;
- (b) make recommendations to public authorities with a view to improving laws and regulations;
- (c) organising support for associations active in the field of gender equality or projects aimed at achieving gender equality;
- (d) to assist, within the limits of its purpose, any person seeking advice on the extent of his/her rights and obligations. This assistance enables the beneficiary to obtain information and advice on how to assert his/her rights;
- (e) to take legal action in disputes relating to the legal mission of the Institute. Where the victim is an identified natural or legal person, action on behalf of that victim shall only be admissible with the victim's consent. Action by the Institute in its own name does not require the consent of an identified victim.

3.2. Prevention in schools: the case of the French Community

In terms of positive law, the prevention measures relating to harassment and cyberbullying mainly concern the sphere of education and in the workplace. Since the latter falls outside the scope of this chapter, this section will focus on prevention measures in the school system. In Belgium's federal system, education falls within the remit of the various language communities. As a result, the rules governing harassment in schools are likely to differ depending on whether we look at the legislation specific to the Flemish, Walloon or German

⁷¹ Loi du 16 décembre 2002, art. 4.

communities, or at the particular case of the Brussels-Capital Region. Rather than detailing each system with its differences and points in common, this section will limit itself to a brief presentation of the existing system for the French Community, as an example of what is practised in Belgium. The reader is invited to bear in mind that differences may exist in other communities.

In a decree dated 15 September 2022,⁷² the government of the French Community defined the guidelines and priority themes for the continuing professional development of members of the educational team in schools and members of staff in psycho-medico-social centres.⁷³ One of the priorities is to develop a positive school climate.⁷⁴ Two of the priority themes included in this guideline relate to the issue of bullying: the prevention and management of conflicts between pupils, the problems of violence and bullying, and the prevention and management/intervention of bullying (including cyberbullying).

A French Community decree was issued on 27 April 2023⁷⁵ aimed at improving the school climate and preventing harassment and cyberbullying at school.

Article 1.7.10-4 of this decree stipulates that the headteacher and the educational team must establish a procedure for reporting and dealing with school harassment and cyberbullying within the school. The aim of this procedure is to detect situations of school harassment and cyberbullying, to refer the pupils concerned and to deal with the situations detected, depending on the skills available and/or the seriousness of the situation, either within the school or with external parties. This procedure must specify the following:

- (a) how the alert is registered,
- (b) the stages in the procedure, from reporting to processing;
- (c) maximum time limits for processing the alert;
- (d) identification of contact persons.

72 Arrêté du 15 septembre 2022 du Gouvernement de la Communauté française fixant les orientations et thèmes prioritaires de la formation professionnelle continue des membres de l'équipe éducative des écoles et des membres du personnel de l'équipe pluridisciplinaires des centres psycho-médico-sociaux pour la période entre les années scolaires 2023-2024 et 2029-2030

73 Psycho-medico-social centres are public services whose aim is to help students achieve their full potential at school and in their personal and social lives; they also look after the well-being and medical care of students. See relevant legislation: <http://www.enseignement.be/index.php?page=24659&navi=2018>

74 Arrêté du 15 septembre 2022, art. 1, 18.

75 Décret du 27 avril 2023 relatif à l'amélioration du climat scolaire et à la prévention du harcèlement et du cyberharcèlement scolaires https://www.gallilex.cfwb.be/document/pdf/51612_000.pdf

The procedure is approved by the organising authority⁷⁶ and is mentioned in the school's internal rules. It is explained to pupils by a member of the educational team at the beginning of each school year. The procedure is regularly communicated by the organising authority or its delegate to all parents, all members of staff at the school and members of the multidisciplinary team at the relevant PMS centre.

The decree of 27 April 2023 creates a framework programme aimed at improving the school climate by preventing and combating school harassment and cyberbullying. It is defined as a programme of actions and support to prevent and deal with bullying and cyberbullying in schools, specific to each participating school.

The schools selected receive a variety of support under the framework programme, such as access to forums for exchanging practices between school professionals, assistance in drawing up or revising the harassment procedure mentioned above, and a range of training courses to help them understand the issues surrounding harassment.

In order to allow a degree of flexibility, the framework programme is made up of three types of action: compulsory minimum actions to be implemented by the participating schools, complementary actions left to the free choice of the schools, and finally additional actions freely proposed by the schools themselves.⁷⁷ The actions in question may be individual, include a group or be collective in nature; they may be structural but can also be ad hoc depending on the needs and issues specific to a particular establishment. However, they must involve pupils as much as possible.

The minimum mandatory actions are as follows:

- (a) Providing training on harassment and cyberbullying;
- (b) Implement conflict management tools, including at least the creation of regulated discussion forums;
- (c) Set up information sessions specifically targeting the issue of cyberbullying, as part of a preventive approach, aimed at all members of staff at the school, as well as parents and pupils;
- (d) Informing parents and pupils about the school's involvement in the framework programme and its content.

⁷⁶ In Belgium, the 'organising authority' (*pouvoir organisateur*) is the authority responsible for organising educational activities in one or more schools. Depending on the type of school (public or private, denominational or non-denominational), it may be a legal entity under public law (local authority) or private law (non-profit association). See Bouttemont, 2004.

⁷⁷ Décret du 27 avril 2023, article 1.7.10-8.

The complementary actions are as follows:

- (a) Setting up an intervention unit made up of people who are trained and authorised to intervene effectively in cases of school harassment or cyberbullying;
- (b) Implementing measures to prevent harassment and cyberbullying in schools, in line with the elements that characterise the school climate.

Additional actions freely proposed by the school are actions contributing to the prevention and management of bullying and cyberbullying at school and to improving the school climate that do not fall within the scope of the minimum or complementary actions already mentioned.

3.3. Platform liability and the case of cascading liability (responsabilité en cascade)

Pending the effective implementation of the European DSA (Digital Services Act) regulation of 19 October 2022, the liability regime for online platforms in Belgium derives from Directive (EU) 2018/1808 of 14 November 2018.⁷⁸ As media regulation falls within the remit of the linguistic communities, each community has its own regulatory authority and its own legislative text. In the case of the French-speaking community, for example, Title IV of a 2021 decree⁷⁹ sets out the provisions applicable to hate speech.

Service publishers may not publish any programme or broadcast any commercial communication that undermines respect for equality between women and men or contains or incites discrimination, hatred or violence based on sex or related criteria such as pregnancy, maternity, gender reassignment, gender expression or gender identity, or contains incitement to violence against women or domestic violence. The same prohibition applies to content containing or promoting discrimination or inciting discrimination, hatred or violence, in particular on grounds of nationality, alleged race, skin colour, descent or national or ethnic origin, age, sexual orientation, religious or philosophical belief, disability, marital status, birth, property, political conviction, language, current or

⁷⁸ Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 <https://eur-lex.europa.eu/legal-content/FR/TXT/?uri=CELEX:32018L1808>

⁷⁹ Décret du 4 février 2021 relatif aux services de médias audiovisuels et aux services de partage de vidéos <https://www.csa.be/wp-content/uploads/2021/03/Nouveau-decret-SMA-du-4-fevrier-2021-Publication-au-MB.pdf>

future state of health, physical or genetic characteristic, social origin or trade union membership.⁸⁰

Any video-sharing service provider must take appropriate measures to protect users from programmes and videos created by users in the situations mentioned above.⁸¹ The measures consist firstly of including the prohibitions in the general terms and conditions of use of the video-sharing service, and making available to the user a system for notifying the video-sharing service provider, according to a simple classification, of prohibited content and informing the user of the action taken by the provider in response to this notification. The service provider must make available to the user a procedure for handling and resolving complaints relating to the implementation of the reporting procedure. It must also take media education measures to make the user aware of these measures. The video sharing service provider shall ensure that these measures are transparent, user-friendly, easy to use and effective. Any video-sharing service provider must set up an internal mechanism for settling disputes with its users. This mechanism must enable disputes to be settled impartially and must not deprive the user of ordinary means of redress. Appropriate measures must take into account the nature of the content in question, the harm it could cause, the characteristics of the category of persons to be protected and the rights and legitimate interests at stake, including those of the providers of video-sharing services and those of the users who created the content or put it online, as well as the general public interest. In accordance with a principle of proportionality, the most harmful content is subject to the strictest access control measures.

The main originality of the Belgian system in terms of liability lies once again in the specific case of press offences. Under Article 25(2) of the Constitution, where the author is identified and domiciled in Belgium, the publisher, printer or distributor cannot be prosecuted.⁸² This means that the publisher, printer or distributor, successively, escape all liability for the writings they publish and distribute, if the author is known and domiciled in Belgium. The purpose of this provision is to protect the freedom of the press and prohibit censorship. It aims to prevent press auxiliaries from being tempted, for fear of a liability lawsuit, to put pressure on authors to modify their writings, or to refuse them assistance. This constitutional rule therefore encourages publishers and distributors not to interfere in the work of journalists, and if they do interfere, they assume their share of responsibility.⁸³ By giving publishers, printers and distributors the privilege of

⁸⁰ Décret du 4 février 2021, art. 2.4-1.

⁸¹ Décret du 4 février 2021, art. 2.4-2.

⁸² Belgian Constitution, art. 25, para. 2.

⁸³ Joachimowicz, 2023.

being able to avoid all liability, both civil and criminal, when the author is known and domiciled in Belgium, it restricts the application of article 1382 of the Civil Code. It therefore constitutes an exception to the ordinary law of civil liability. According to the Court of Cassation's constant jurisprudence,⁸⁴ liability cascading liability applies both on criminal as well as civil proceedings.⁸⁵

The rule of cascading liability does not apply to providers of intermediary online services, such as internet service providers, online platforms, search engines, social networks (Facebook, X (ex-Twitter), Instagram, etc.). Under certain conditions, and for some of their activities, they benefit from a separate liability exemption regime, which is based on section 4 of a European Directive from 2000⁸⁶ (eCommerce Directive), transposed into Belgian domestic law in Book XII of the Economic Law Code.⁸⁷ The eCommerce Directive was amended by Regulation (EU) 2022 on a single market for digital services.⁸⁸ Article XII. 19 of the Code of Economic Law and Article 6 of the DSA introduce a conditional exemption from liability. The host is not liable for information stored at the request of a recipient of the service provided that it does not have actual knowledge of the unlawful activity or information, or, in the case of a civil action for damages, of facts or circumstances from which the unlawful nature appears; or that it acts promptly, as soon as it has actual knowledge, to remove the information or block access to it and provided that it immediately informs the Public Prosecutor.

The host may itself become aware of the illegal nature of the content it is hosting, or may be informed of this by a third party asking it to remove the content or block access to it. It is therefore up to the host to assess whether or not the information is illegal. If he leaves the information and it is illegal, he is liable. If he deletes it and it is legal, he infringes the freedom of expression of the author of the information. He thus takes on the role of private censor of sorts. He can also contact the content provider and ask him to voluntarily remove the illegal information.

⁸⁴ Cour de cassation, 31 May 1996.

⁸⁵ Berbuto, Thevissen, 2021.

⁸⁶ 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.

⁸⁷ Code de droit économique, art. XII.1 to XII.23 https://www.ejustice.just.fgov.be/img_l/pdf/2013/02/28/2013A11134_F.pdf

⁸⁸ Regulation (EU) No 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a single market for digital services.

In practice, intermediaries set up procedures for reporting abuse and confine themselves to deleting illegal content in the event of flagrant infringement of intellectual property rights or personality rights.

The absence of a general obligation to monitor does not preclude intermediaries from being subject to specific injunctions from judicial authorities, which may impose a temporary monitoring obligation on them in a specific case, where this possibility is provided for by law.⁸⁹ Thus, for example, the CJEU considers that social networks may be subject to a judicial injunction to block access to certain stored information whose content has been deemed unlawful or to remove the unlawful content. Such an injunction is not considered to impose on the social network concerned a general obligation to monitor the data it stores or to actively seek out unlawful content.⁹⁰

Under Articles 9 DSA and XII.20, § 2, of the Code of Economic Law, as soon as an injunction to take action against specific illegal content is received from the competent national judicial or administrative authorities, the intermediary is required to inform them as soon as possible of any action taken.⁹¹

Intermediaries are obliged to inform the competent judicial or administrative authorities without delay of the alleged unlawful activities of the recipients of their services, or of the alleged unlawful information supplied by them. They must also communicate to the judicial or administrative authorities, at their request, all information relevant to the investigation and establishment of offences committed through their intermediary. Judicial injunctions must strike a fair balance between the rights and interests at stake: the protection of personal data, the protection of intellectual property rights, freedom of expression and communication, including the freedom to receive information and freedom of enterprise.⁹²

Summary

Belgium has a mixed legal landscape when it comes to regulating hate speech and cyberbullying. In terms of legislation, the country has, in principle, fairly comprehensive legislation to deal with contemporary issues. Three main laws

⁸⁹ Code de droit économique, art. XII.20, § 2.

⁹⁰ CJEU, 3 October 2019, Case C-18/18 *Glawischnig-Piesczek*.

⁹¹ Code de droit économique, art. XII.20, § 2.

⁹² CJEU, 29 January 2008, Case C-275/06, *Productores de Musica de Espana (Promusicae) v Telefonica de Espana SAU*.

were passed successively from the early 1980s to the early 2000s, and have been regularly updated since then. They aim to combat racism and discrimination and to promote equality between men and women. These laws provide a fairly comprehensive legal framework (albeit a somewhat fragmented one) to protect victims and penalise the perpetrators of hate speech and harassment, in theory at least.

In practice, the constitutional provisions relating to press offences, which were originally intended to protect press freedom, result in *de facto* impunity for a large proportion of offences. Since a constitutional reform in 1999, crimes of opinion committed with racist or xenophobic motives have been excluded from the special regime for press offences. Moreover, the concept of press offence itself has been interpreted in what might be described as an originalist way by the Court of Cassation. As a result, the audiovisual media are excluded from the constitutional protection applied to the press. Anti-discrimination bodies have regularly protested against this breach of equality, but as they have not been able to muster the two-thirds majority required for a constitutional revision, no project has yet come to fruition.

Another limitation of the current system is to be found in the federal nature of the Belgian system and its administrative fragmentation, with legislation falling within the remit of the federated entities sometimes suffering from a lack of legibility. This is particularly the case in areas such as media regulation and the prevention of bullying in schools.

At the institutional level, the country has gradually built up institutions over the last few decades to support the fight against discrimination. These tasks include producing documentation to provide information to the public authorities and to victims of discriminatory acts. The bodies that provide this information also have the task of offering alternatives to legal proceedings, which seems particularly appropriate in the case of acts that are harmful but can potentially be remedied without involving the criminal justice system.

Bibliography

- Berbuto, S., Thevissen, P. (2021) 'Presse', Postal Mémoires Lexique du droit pénal et des lois spéciales, p. 1–51
- de Bouttemont, C. 'Le système éducatif belge', Revue internationale d'éducation de Sèvres, 37 | 2004, pp. 101–108.
- Carneroli, S. (2021) 'La cour d'assises de Liège se mobilise pour juger un délit de presse inspiré par le sexisme. Vers la fin de l'impunité pénale?', Auteurs & Médias 2021/4 393–394
- Colette-Basecqz, N. (2018) 'La responsabilité pénale liée au phénomène du cyberharcèlement et à ses différentes formes d'expression' in Jacquemin, H. (coord.), Responsabilités et numérique, Limal, Anthemis, pp. 35–61
- Commission d'évaluation des lois fédérales tendant à lutter contre la discrimination (2022) Rapport final – Combattre la discrimination, les discours de haine et les crimes de haine: une responsabilité partagée [Online]. Available at: <https://equal.belgium.be/fr/actualites/rapport-final-de-la-commission-de-valuation-des-lois-federales-tendant-lutter-contre-la>
- Hugon, C. 'Pour une révision de l'article 150 de la Constitution: une nécessité de cohérence, d'égalité et d'effectivité dans le traitement judiciaire des discours de haine', in Englebert, J. (coord.), La régulation des contenus haineux sur les réseaux sociaux, coll. Débats & Droit, Anthemis, Limal, 2022, p. 142
- Joachimowicz, A. (2023) 'La responsabilité civile des médias – La liberté de la presse et d'expression dans la Constitution belge' in Responsabilités. Traité théorique et pratique, Livre 26bis. 1–27
- Lambert, P. (2020) 'Génocide – Crime contre l'humanité' Postal Mémoires. Lexique du droit pénal et des lois spéciales, G 20 / 01 – G 20 / 14
- Leroux, O. (2016) 'Criminalité informatique' in Beernaert, M.-A. (e.a.), Les infractions – Volume 1. Les infractions contre les biens, 2nd edition, Brussels, Larcier, p. 512
- Milecan, G. (2021) 'Le délit de presse aux assises', Journalistes n°240, October 2021, pp. 4–6. [Online] Available at: <https://www.ajp.be/wp-content/uploads/2022/02/240Dossier.pdf>
- Mincke, C. (2010) 'La médiation pénale: mécanismes et promesses', La médiation pénale face à ses idéaux fondateurs. De l'utopie à l'aveuglement, pp. 5–59
- Mouffe, B. (2014) 'Restrictions et limitations générales au droit à la liberté d'expression du journaliste', La responsabilité civile des médias, pp. 52–169
- Rosoux, G. (2005) 'Brèves considérations sur l'obsolète notion de délit de presse...', Revue de Droit Pénal et de Criminologie, pp. 1270–1289

- Van De Kerchove, M., Cartuyvels, Y., Guillain, C., Tulkens, F. (2014) 'La définition de l'infraction – La classification des infractions' in Introduction au droit pénal. Aspects juridiques et criminologiques, pp. 331–368
- Vrielink, J. (2022) 'Contre l'impunité de fait des délits de presse confiés au jury d'assises (art. 150 const.): quelles pistes choisir?' in X. Delgrange (coord.) Les Cahiers du C.I.R.C., no. 5, June 2022, p. 52
- Thevissen, P., Werding, A. (2022) 'Harcèlement' in Postal Mémorialis. Lexique du droit pénal et des lois spéciales, H 15 / 01 – H 15 / 27

XVIII. LIBERTÉ, ÉGALITÉ... ET FRATERNITÉ? COMBATING HATE SPEECH AND CYBERBULLYING IN FRANCE, HOME OF THE ENLIGHTENMENT

PÉTER SZÓKE

Combating cyberbullying is an uphill battle which must be fought even against all odds. The evolution of the relevant French laws has so far produced an intricate web of formally *sui generis* norms which revise and update one another and the end of the road is not in sight. This reflects a reactive approach: a rapidly changing technological and social environment gives rise to a rapidly changing, increasingly complicated and detailed legal environment. In the view of this writer, French lawmakers could as well have chosen a different path: a solid, elaborate dogmatic framework provided for by the Press Act and the Penal Code with only rare amendments in case of compelling necessity so as to leave the rest to judicial practice.

1. Striking a delicate balance: hate speech in physical and virtual space

1.1. Introductory remarks: to punish or not to punish

Hate speech as such is a new category and a new offence. Different legal systems deal with it differently. Some seem hardly to bother at all. The US Supreme Court, e.g. has deduced from the First Amendment an obligation of neutrality

https://doi.org/10.47079/2025.kprhk.cyberb.4_19

between points of view, which should preclude the prosecution of hateful expressions. But the absence of penal repression does not mean passivity. Public authorities can denounce and criticize hate speech and start a counter-discourse or allow and even encourage other players to do it. And it is not penal law only that can be deployed in the fight. Administrative and civil law can furnish the state and the public with important tools. Disciplinary measures can be taken against subjects, such as professors or journalists, who abuse their position to spread hatred and contempt against segments of society. TV channels violating anti-discriminatory laws or the terms of their license can be taken off the air.¹

Interestingly, the approach of the European Court of Human Rights (ECHR) is not very dissimilar from that of the Supreme Court. The repression, even penal, of any abuse of freedom of expression should, by definition, not be problematic. However, the ECHR usually takes a different line. It sees the incrimination of an expression more often as a limitation on freedom of expression and questions its justifiability. And justification seems to be more difficult to establish when the disputed measure is of penal nature. For the ECHR, a criminal conviction is “one of the most serious forms of interference with the right to freedom of expression”.² In fact, the Strasbourg case law has shown its preference for non-penal measures, if available, against hate speech like offences.³

The ECHR is, needless to say, even more reluctant to go along with prison sentences for speech related offences. Prison sentences should in principle be excluded in matters of freedom of expression. A prison sentence for a press offence is compatible with the freedom of journalistic expression guaranteed by Article 10 of the European Convention on Human Rights only in exceptional circumstances⁴, where the impugned remarks incite the use of violence against an individual, a representative of the State or a section of the population. Today, French courts are rather cautious when it comes to condemning such speech, let alone imposing prison sentences. A conservative jurisprudence tends to require that the disputed expression be sufficiently explicit, or that it apply to all members of the group,⁵ as demonstrated by the acquittal of Éric Zemmour by the Paris Court of Appeal, to which I shall return in due course.

1 Hochmann, 2024, pp. 2–3.

2 ECHR, *Perinçek v. Switzerland*, 15 October 2015, § 273. For more recent see ECHR, *Halet v. Luxembourg*, 14 February 2023, § 150., cit. by Hochmann, 2024, p. 3.

3 Hochmann, 2024, p. 4.

4 ECHR, *Cumpăna et Mazăre v. Romania*, § 115. 17 December 2004.

5 Hochmann, 2022, p. 4.

1.2. *From Voltaire to anti-racist legislation*⁶

Many have said and written that, of the threefold constitutional motto of liberty, equality and fraternity, it is to the last to which France issuing has been able to live up the least. The country has seen not one but several bloody revolutions. But France has always been a laboratory of new ideas, a political culture in constant turmoil, a political culture honed between sharp intellectual contrasts, a world of republican patriots versus nationalist collaborators with the Third Reich, of revolutionaries versus uncompromising conservatives, a world divided between a high European culture and immigrant subcultures with varying degrees of social integration. The understanding of French legislation may also be of particular interest, as France is a cradle of the constitutional and legal guarantee of modern freedom of expression. In a 1984 decision, the Constitutional Council (Conseil constitutionnel) affirmed that freedom of expression is fundamental, precious not only in its own right, but also as the guarantee of other human and civil rights, and even of national sovereignty.⁷ Thinkers of the French Enlightenment played a pioneering role in the development of the concept and in the recognition of freedom of expression and opinion as a fundamental right, the universality of which would be difficult to contest. The passionate attitude of the French towards the right to freedom of expression is well illustrated by the bon mot attributed to Voltaire, although perhaps apocryphal: 'I disapprove of what you say, but I will defend to the death your right to say it'.

The French constitutional basis for action against hate speech is still founded on the balance already struck in the Declaration of the Rights of Man and of the Citizen, which forms part of the current Constitution.⁸ Nowhere is, for that matter, a definition of hatred in French law to be found. So the legislator targets hatred without ever defining it. The specificity of this legislation is that the important substantive provisions relating to criminal liability are not exclusively, or even primarily, contained in the Penal Code (Code pénal),⁹ but in the 1881 Act on the Freedom of the Press¹⁰ ('Press Act') and subsequent legisla-

6 For a brief historical overview of French legislation on freedom of expression, see Vilard, 2001, pp. 137–148.

7 Cons. const., Oct. 10–11, 1984, no. 84–181 DC.

8 Constitution du 4 octobre 1958.

9 Penal code. In French law, the major codes have no number. Some codes are not codifications but compilations, i.e. a constantly evolving collection of the main rules in force in a given field of law. The drafting of this chapter encountered a particular difficulty: we had to decide in each case whether to give as the legal reference the relevant provision of the basic law, such as the Penal Code, or the law which amended it, or both.

10 Loi du 29 juillet 1881 sur la liberté de la presse.

tion, which has become necessary due to the emergence of new media and the changes in the social fabric of the nation.

Chapter IV of the Press Act is entitled ‘Crimes and offences committed through the press or any other means of information’.¹¹ Article 29 defines two basic offences: defamation (diffamation) and insult (injure). Defamation is ‘any allegation or imputation of a fact that is prejudicial to the honour or reputation of the person or body to which the fact is imputed..... The direct publication or reproduction of this allegation or imputation is punishable, even if it is made in ambiguous (dubitative) form or if it refers to a person or body not expressly named, but whose identification is made possible by the terms of the incriminated speeches, cries, threats, writings or printed matter, placards or posters’. Insult is ‘any offensive (outrageante) expression, term of contempt or invective that does not imply the imputation of any fact’. The distinction is, therefore, possible by the presence or the absence of a statement of or reference to a fact. This implies the *exceptio veritatis* principle developed by French case law. If the accused can prove that he acted in good faith, reasonably believing that the contested statement was true, then he may see the charges against him dropped. Needless to say that the case law struggles to set standards by which the exception of truth can be established.¹² Both insult and defamation have to be committed in public to trigger criminal prosecution. If they are committed in private, they may constitute a mere contravention subject to an administrative sanction, possibly a fine. In 2013, e.g. the French Supreme Court (Cour de Cassation) ruled that an employee’s remarks posted on Facebook against his superior, however offensive they might be, did not constitute a public insult if the viewership of the post is restricted to the ‘Facebook friends’ of the offender.¹³

The amendments to the Press Act reflect the changes that have taken place in the norms governing criminal responsibility for opinions over the last one hundred and forty years. It is worth recalling a rare episode from the legal history of interwar Europe. While some other European countries were passing anti-Jewish laws, the Daladier government attempted to combat racist propaganda with a decree-law promulgated on April 21, 1939. This was the ‘Marchandeau Decree’, which amended the Press Act, punishing with imprisonment anyone seeking to discredit (defamation) a person or group of people on the grounds of their race or religion, in order to excite hatred against them among

11 On some occasions, the Penal Code itself refers to it, e.g. in Article 132-76.

12 The fact has to be precise for the court to establish responsibility for defamation. Letteron, 2023, pp. 525-532 cites extensive case law on insult and defamation based on article 29 of the Press Act.

13 Civ. 1ère 10 avril 2013 cit. in Letteron, 2023, p. 525.

citizens or the general public.¹⁴ The term ‘race’ appeared for the first time in French law; however, unlike elsewhere in Europe, the French legislator’s intention was not to persecute but to protect an embattled minority then. It was in the same spirit that Article 1 para 1 of the 1958 French Constitution mentions again ‘race’: in fact, it guarantees the ‘equality without distinction on the basis of origin, race or religion before the law’. After the Second World War, France adopted its first ‘anti-racist’ legislation as early as 1972, way ahead of other European countries. It is commonly known as the ‘Pleven Law’.¹⁵

The French lawmakers have chosen to reaffirm and apply the traditional freedom of expression to cyberspace by way of a *sui generis* new legislation, instead of adapting the Press Act and the Law on Audio-visual Communication¹⁶ to the new realities. In 1986, Article 1 of the Léotard Law declared that ‘communication to the public by electronic means is free’; the same article makes it clear that the purpose of the law is to apply the freedom of expression to cinema, radio and television.¹⁷ Soon, the legislator found it necessary to extend the scope further still, i.e. to the Internet. Once again, he did this not by way of amendments but of new legislation, namely by Act 2004-575 on confidence in the digital economy (LCEN).¹⁸ Its Article 1 repeated the principle of the freedom of expression in online communications. However, both laws, in their respective first articles, drew limits: ‘The exercise of this freedom may be limited [...] by respect for human dignity, the freedom and property of others and the pluralist nature of the expression of schools of thought and opinion and, on the other hand, by the protection of public order, national defence requirements, public service requirements, the technical constraints inherent in the means of communication and the need for audio-visual services to develop audio-visual production.’¹⁹

14 ‘...exciter à la haine entre les citoyens ou les habitants’. The original text of the legislation is not available on Légifrance, the official data base of French legislation but only on Gallica, which archives official journals: <https://gallica.bnf.fr/ark:/12148/bpt6k6550948q/f3.item#>.

15 Loi n° 72-546 du 1 juillet 1972 relative à la lutte contre le racisme. Pleven was the Minister of Justice who proposed the draft. In France, laws are often and informally named after the person who proposed the draft.

16 Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle.

17 Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication (Loi Léotard).

18 Loi n° 2004-575 du 21 juin 2004 pour la confiance dans l’économie numérique.

19 This is in line with the Declaration of the Rights of Man and of the Citizen: freedom is enshrined and guaranteed, but within the limits set by the law. The latter is the origin of Liberty, its source and its limit that form, all rolled up into one, the French concept of *légicentrisme*. It means that the law is central and perfect as the expression of the general will. At least, it was regarded as such until 1958, the creation of the Constitutional Council, which alone has the power of check and sanction laws against the Constitution.

1.3. New minorities: extending protection in post-colonial France

However, the Marchandeau decree, which was repealed in 2011, had proved inadequate to deal with the new tensions. For one thing, it was difficult to enforce in the courts. It was never easy to prove that incitement to hatred was the purpose of committing an act, so the courts seemed ready to tolerate a ‘moderate racism’ of sorts. Thus, e.g., in 1952, a few years after the Holocaust, a Paris court acquitted a man who had called for ‘just laws against the exploitative activities of the Jews against our people’ and for ‘moderate and reasonable anti-Semitism’.²⁰ After the Algerian civil war and the liberation of the French colonies, the proportion of people of North African and sub-Saharan origin in the French population increased, and with it the atrocities, discrimination and even crimes against them. Among the perpetrators were far-right groups opposed to Algerian independence, paramilitary groups, but also ordinary citizens: concierges, landlords, cab drivers, gendarmes, etc. On the other hand, civil rights campaigners would demand decisive action from the state to protect minorities, claiming that racially-motivated or xenophobic crimes often went unpunished; in other words, there was a suspicion that racism had contaminated the justice system and had become endemic.²¹ Prior to the adoption of the Pleven Law, there was an extensive public debate on the appropriateness of a distinction between specific categories of victims and on the necessity of adopting a *lex specialis*. Sceptics asked whether it would not violate the principle of equality if the legislator were to tell the judge how to interpret a crime committed against members of a particular ethnic or religious group, while for other groups the general rules of criminal law would continue to apply. The turning point came after France ratified the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD), adopted by the UN General Assembly in 1965, and the ensuing legislative obligation. The Pleven Law of 1972²² added an anti-racist clause to Article 24 of the Press Act, prohibiting discrimination and incitement to hatred or violence on ethnic, national, racial or religious grounds. It punishes with up to one year in prison and/or a fine anyone who ‘incites discrimination, hatred or violence against a person or group because of their origin or because they belong or do not belong to a particular ethnic group, nation, race or religion’. In this case, the behaviour itself is criminal, even if not ‘effective’, i.e. the incitement is not followed by action.²³ Of course, the incitement can be effective and

20 Hochmann, 2022, p. 2.

21 Brahim, 2020, pp. 237–270.

22 Loi n° 72-546 du 1er juillet 1972 relative à la lutte contre le racisme.

23 Pleven Law Art. 1.

successfully provoke someone to commit a racially motivated crime or offence. In this case, the wrongdoer will be punished as accomplice to the action classified as crime or offence under the Penal Code and the severity of the punishment will vary accordingly. The provocation must happen ‘either by speeches, shouts or threats uttered in public places or gatherings, or by writings, printed matter, drawings, engravings, paintings, emblems, images or any other means of any other written, spoken or pictorial material sold or distributed, offered for sale or exhibited in public places or by placards or posters exposed to public view’; it is also necessary that the employment of the aforementioned means will have ‘directly provoked the perpetrator or perpetrators to commit the said action’, if the action was actually carried out.²⁴ It is clear that the establishment of direct causality is required, i.e. the incitement must inevitably lead to the action. The Pleven Law added the definitions of ‘racially motivated insult’ and ‘defamation’, making these two specific offences subject to public prosecution, contrary to the general statutory provisions on insult and defamation, classified as private offences.²⁵

One of the key achievements of the Pleven Law was to allow certain NGOs accredited and registered to combat racism and discrimination to exercise the rights of a private party in ongoing criminal proceedings, with the consent of the victim.²⁶

Yet, not even the Pleven Law did fully meet the expectations. The application of the law was uncertain. Social pressure did not abate, and street demonstrations followed one another: e.g., an association of mothers of the victims of racist crimes organized a mass rally in the spring of 1984 to demand that anti-racist legislation be maintained and, in general, that both lawmakers and law enforcement agencies take tougher action. In the end, they obtained but minor concessions. Law 85-10 of 1985 on certain social provisions went only as far as to widen the scope of NGOs eligible as private parties in criminal proceedings for racist offences.²⁷

The 1980s were marked by an increase in atrocities committed against mainly Arab and African immigrants, but also by a rise in anti-Semitic demonstrations towards the end of the decade. Lawmakers were first confronted with the phenomenon of Holocaust denial after far-right politician Jean-Marie Le Pen

²⁴ Pleven Law Art. 2; Penal Code Art. 121-7.

²⁵ Pleven Law art. 3,4, art. 5. Para I. The more stringent punishment in case of racial motives is also backed by art. R625-8 of the Penal Code.

²⁶ Ibid. art. 5 para II.

²⁷ Loi n° 85-10 du 3 janvier 1985 portant diverses dispositions d'ordre social; Brahim, 2020, p. 6.

referred to the gas chambers as a ‘detail’ of the Second World War.²⁸ The fight against Holocaust revisionism led to the adoption of the Gayssot Law,²⁹ the purpose of which was to suppress racist, anti-Semitic and xenophobic expressions. This law further amended the Press Act and the Penal Code. It introduced the criminal offence of Holocaust denial — a move that remains controversial to this day. Its critics argue that codifying a particular reading of history violates freedom of expression and, by distinguishing the Shoah from other genocides, may compromise the principle of equality. But in 2015 the Constitutional Council rejected both of these criticisms. On the one hand, it found that denying or minimizing the atrocities committed during the Second World War and crimes against humanity condemned as such by international criminal tribunals and French courts constituted racist and anti-Semitic incitement in itself, and on the other, that the text of the norm as intended by the legislator would in no way restrict historical debate. Holocaust denial is an abuse of freedom of expression, and the legislative instrument chosen to prevent it constitutes an appropriate and proportionate restriction on that freedom. The special provisions on Holocaust denial are justified not only by its seriousness but also by its special place in previous national and international legislation and case law: perpetrators of the Holocaust had been tried and the nature and character of their crimes clarified by international and French courts.³⁰ It is interesting to note, however, that the United Nations Human Rights Committee (UNHRC) had already gone further sixteen years earlier in *Faurisson v. France*. It concluded that a challenge to the infallibility of the International Tribunal of Nuremberg would not in itself have created a sufficient basis for restricting freedom of expression; the decisive argument to convince the UNHRC was that Faurisson, who had been convicted in France under the Gayssot Law, had expressed his revisionist views not as a researcher, in an academic debate, but through hate speech.³¹

The ensuing debate focused on the appropriateness of introducing racist, anti-Semitic and xenophobic motives as a general aggravating circumstance in penal law. Legislators hesitated for a long time, but at the turn of the millennium the situation became so serious that they felt compelled to act. Once again, some external causes were to blame for the rise in racial and ethnic antagonism: the escalation of tensions in the Middle East, the terrorist attacks on 9/11 and

28 Available: <https://www.dailymotion.com/video/x2m2xr4>

29 Loi n° 90-615 du 13 juillet 1990 tendant à réprimer tout acte raciste, antisémite ou xenophobe.

30 Decision no. 2015-512 QPC du 8 2016.

31 Robert Faurisson v. France, Communication No. 550/1993, U.N. Doc. CCPR/C/58/D/550/1993(1996). Available at: <http://hrlibrary.umn.edu/undocs/html/VWS55058.htm>; Kondorosi, 2015, p. 83.

the wars launched by the United States and its allies in response, radicalized certain sectors of the French Muslim minority, but also the anti-immigration political movements. Two deputies from the Gaullist ruling party in the National Assembly declared that the frequency and nature of anti-Semitic and Islamophobic incidents were already reminiscent of the atmosphere of the interwar period.³² It was also during these years that the European Union took an interest and adopted legislation to combat racism, xenophobia and anti-Semitism. Law no. 2003-88³³ finally introduced ethnic, national, racial or religious hatred as a general aggravating circumstance in the Penal Code. The existence of an aggravating circumstance may be established by the court if the wrongdoing is preceded, accompanied or followed by a verbal, visual, material or other manifestation that offends the honour or consideration of the victim because of his or her belonging or not belonging to a particular ethnic group, nation, race or religion. The relevant provision of the law establishes categories according to the punishments threatening the general offences and defines the measure of the aggravation of the punishment in each category if the offence is accompanied by an expression of racial hatred. Thus, e.g., 30 years' imprisonment is changed to life, 20 years to 30 years in prison, etc.³⁴ In January 2017, in a separate article sex, sexual orientation or gender identity were added to the catalogue. The tendency is clear: the lawmaker wants to take an increasing number of minorities under his protective umbrella.³⁵

1.4. New fronts open up: the battle continues in cyberspace

As we have seen, the Press Act has been continually updated over the decades. As a result, it is increasingly pointless to distinguish between offline and online means of combating hate speech. The current wording of the Press Act already extends the scope of the law to journalists publishing on the Internet³⁶. In general, it is safe to say that there is no such thing as *sui generis* cybercrime, but only crimes and offences committed via the Internet. Most of these were known before the advent of the Internet, but there are types of crimes that are easier to commit in cyberspace. Thus, the Internet is just the 'medium', nothing more and nothing less.³⁷

³² Brahim, 2020, p. 10.

³³ Loi n° 2003-88 du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xénophobe.

³⁴ Penal Code art. 132-76.

³⁵ Penal Code art. 132-77.

³⁶ Press Act art. 2.

³⁷ Letteron, 2023, p. 532.

An important legislation in the fight against hate content in cyberspace is the LCEN. It contains basic provisions on the possibilities for co-operation and action against hateful content, and the liability of content providers and online platform operators. The most important rules are set out in Article 6 of the LCEN and its supplements. The legislator has regulated material on three levels. Firstly, he has defined the civil and criminal liability shared between the Internet service provider (ISP, *hébergeur*) and the content publisher (*éditeur*). Secondly, he has defined and sanctioned situations and behaviours in which hateful content constitutes a threat to public order. In such cases, the norm imposes a duty of vigilance on the ISP. The third layer or level targets particularly serious offences such as child pornography or terrorism.

The lawmakers now considered this legislation outdated — there were no smartphones or social media at the time of its adoption — and moved to strengthen liability by passing the Avia Law in 2020.³⁸ The Avia Law would have imposed stricter responsibilities and obligations on operators of online platforms and search engines to remove hate content almost immediately after an alert. This rule never entered into force as the Constitutional Council declared all but one provisions of the Avia Law unconstitutional. Eventually, a new legislation to address constitutional concerns was passed in August 2021. This was the Law Reaffirming Respect for the Principles of the Republic,³⁹ which sought to draw the consequences from the fiasco of the Avia Law. The original aim of this law was to combat separatism, which is why it is referred to in the literature as ‘Separatism Act’.⁴⁰ Title I aims to guarantee coherence with the principles of the Republic and the minimum requirements of social life. Its provisions include rules on hate speech and harmful content on the Internet. The provisions of Chapter IV are so comprehensive that they are often regarded as ‘a law within a law’.⁴¹ It amends the Penal Code, the Code of Criminal Procedure, the Press Act, the Léotard Law, the LCEN and the Code of Education.⁴²

The lawmakers wanted to react to terrorist and hate crimes that were threatening the constitutional order, such as the attack on the editorial office of *Charlie Hebdo*, or the murder of high school teacher Samuel Paty in broad daylight in the fall of 2020. Mr. Paty had been targeted by Muslim extremists on social media, who virtually condemned him to death after he taught his students how to defend freedom of expression even in the face of the outrage provoked by the

38 Loi n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet.

39 Loi n° 2021-1109 du 24 août 2021 confortant le respect des principes de la République.

40 Bigot, 2021, p. 8.

41 Bigot, 2021, p. 1.

42 Code de l'éducation.

Mohammed cartoons of Charlie Hebdo. After his assassination, he was widely considered the victim of ‘doxing’, the practice of seeking out and disclosing private or identifiable information about a person on the Internet with the intention of harming him. Lawmakers now decided to combat doxing by introducing a new provision in the Penal Code that criminalizes the disclosure, dissemination or transmission of personal data or information, whether off- or online, with the aim of identifying the victim or members of his or her family and thereby exposing them to imminent risk of assassination. The penalty is three years’ imprisonment and a fine of 45,000 euros. The offence entails a harsher punishment if committed against a public official, a journalist, a minor or a person with one of the vulnerabilities listed in the provision. If a printed, audio-visual or online publication has been used to commit the offence, criminal liability must also be established in accordance with the rules governing the publisher’s or operator’s liability.⁴³ This provision was also challenged before the Constitutional Council on the grounds that this penal provision could hinder the establishment of facts by journalists against public figures or law enforcement agencies abusing authority. However, in August 2021, the Council upheld the provision, arguing, i.a., that the disclosure of personal data only constitutes a criminal offence if it is intended to deliberately and directly endanger the victim;⁴⁴ journalistic activities will therefore not be subject to this penal provision.

The offender is punishable if found guilty of these four elements:

- a) Information or data is revealed, diffused or transmitted, whether off- or online. In this way, the legislator wanted to keep up with the times and go beyond the paradigm offered by the Press Act.
- b) The information concerns the victim’s either private or professional life. Here too, the legislator wanted to avoid the often contentious debate on the limits of privacy;
- c) The information enables the offender to identify and locate the victim: this is the most important requisite which helps us understand why the first two concepts are defined so broadly.
- d) Motive: a *sine qua non* for establishing criminal responsibility. This offence cannot be committed through negligence. It must be proved in court that the purpose of the act was to expose the victim, his family or his property to a ‘direct risk of harm’.
- e) It must be a danger that the author could not have been unaware of.⁴⁵

⁴³ Art. 223-1-1 of the Criminal Code.

⁴⁴ Cons. const., 13 août 2021, n° 2021-823 DC.

⁴⁵ Bigot, 2021, p. 12.

The only provision of the Avia Law untouched by the Constitutional Council provided for the establishment of an Observatory of online hate speech (*Observatoire de la haine en ligne*)⁴⁶. The Observatory, today functioning as part of the Audio-visual and Digital Communications Regulatory Authority (ARCOM)⁴⁷ monitors and analyses hate content on the Internet, particularly on social media to whose role and powers.

1.5. The rules in force

Before turning to jurisprudence on hate speech and then to the issue of cyberbullying, let's review and set out the key elements of existing hate speech legislation and related offences in light of what has been said so far.

Article 23 of the Press Act contains a general penal clause limiting the freedom of the press, to prevent it from being abused to facilitate the commission of crimes. Any person is liable as an accomplice who directly provokes the commission of a crime by

- a) comments or threats made in public or in a public place;
- b) in written, printed or illustrated form, if they are sold or displayed in a public place, e.g. on a poster, or
- c) electronically.

It is important to note that any incitement must be followed by effect for the act to be punishable. By contrast, Article 24 of the Press Act criminalizes all acts which, by abusing the means of free public expression, incite the commission of specific violent crimes against human life and dignity and crimes against the interests of the nation (treason), even if the incitement is not followed by effect. This is the link between the different 'generations' of amendments to the Press Act and the Penal Code: if the incitement is effective, i.e. if it actually triggers one of the offences mentioned, the act is already covered by the general part of the Penal Code⁴⁸. More relevant to our subject is the above-mentioned article 24 of the Press Act, which imposes the same penalty on anyone who justifies (*fait l'apologie*) of

- a) war crimes or crimes against humanity, or
- b) slavery
- c) cooperation with the enemy,

46 <https://www.csa.fr/Informer/Toutes-les-actualites/Actualites/Observatoire-de-la-haine-en-ligne-analyser-pour-mieux-lutter>

47 Autorité de régulation de la communication audiovisuelle et numérique.

48 Penal Code art. 121-7.

even if the perpetrators of the acts justified or condoned have never been convicted for the simple reason that their acts were not considered criminal under the laws of the time but would be subject to prosecution and moral indignation now. These latter provisions may be understood in light of France's colonial past or by some events of the Second World War. In fact, some segments of the public cherish nostalgia for colonial gloire and their relationship with the Vichy regime also remains ambiguous.

If we look for the current definition of hate speech, then Article 24 might be a candidate. It states that anyone who incites discrimination, hatred or violence against a person or group on the grounds of their origin or belonging or not belonging to a particular ethnic group, nation, race or religion is liable to a prison sentence of up to one year and/or a fine. In the same way and in another paragraph of the same article, the law threatens to punish anyone who commits the above-mentioned offences against a person or group because of the victim's gender, sexual orientation, identity or disability. The punishment is harsher if the perpetrator is a person exercising public authority or a public function, and commits the offence in that capacity. It is important to note that there is no criterion of effectiveness, i.e. the incitement does not have necessarily to result in action in order to be punishable. It should be remembered that Article 24, as it stands, is the product of a long evolution in which the legislature has sought to extend protection to more and more categories. A case in point is gender and sexual orientation for which one can become the victim of hate crimes. However, the attentive reader will have noticed that the definition is not that of hate speech. There is no general prohibition of hate speech in French law as the legal system cannot impose the obligation on anybody to love or not to hate somebody. One can rather speak about 'hate speeches' in plural rather than 'hate speech' in singular. What they all have in common is that they target a person or a group not for what they do but for what they are.⁴⁹

Articles 32 and 33 of the Press Act govern the offence of defamation. Defamation may be directed against an individual or group on the grounds of their belonging or not belonging to a particular ethnic group, nation, race or religion. The offence is punishable by a fine and/or imprisonment. In the same article, the legislator also provides for the punishment of insult based on gender or identity, sexual orientation or disability.⁵⁰ The court may order the offender, if found guilty, to exhibit or publish the sentence in whole or in part or to publish

⁴⁹ Laslier, 2024, pp. 1–2.

⁵⁰ Here too, the scope of protected persons has been extended by the law on separatism.

it, even in the *Journal officiel de la République française*⁵¹. With regard to discrimination, the article refers to the definition in the Penal Code⁵².

Under Title III of Book I of the Penal Code, among the aggravating circumstances, it is provided that if the offence is preceded or accompanied by hate speech, the penalty is increased according to a scale. The aim of the Penal Code is to avoid the need to prove causality in court. The aggravating circumstance can therefore take on two forms. The offender has uttered insults (visual, verbal, etc.) against the victim on the grounds of race, nationality, ethnicity, religion, gender or sexual orientation, which

- a) were directed against his or her honour or reputation, or
- b) it is proven that the victim's affiliation or orientation was the motive, as described above.

However, to complicate matters further, the Criminal Code, in its special part, in the case of the crime of aggression (violence), also separately mentions, among its various elements, qualified cases in which the violence is committed because of the victim's identity or because he or she belongs or does not belong to one of the above-mentioned categories.⁵³

1.6. Hate speech between penal law and press law⁵⁴

The relationship between the Press Act and the Penal Code is complex and not easy to understand. In olden days, defamation and insult would typically target some individual citizen or public figure. Today's expressions of contempt are meant to injure entire categories or communities of persons thus threatening the fabric of democratic society and peaceful convivence with disruption. Successive legislators have strengthened the penal sanctions attached to this type of speech. These developments have given rise to a system of laws designed to suppress hate speech. It includes a gradual extension of the statute of limitations for hate speech offences and an increase in penalties. As to the former, the original statute of limitations under Article 65 for press offences was only three months based on the idea of the 'right to forget' (*loi d'oubli*): the rapid circulation of expressions should effectively chase away the memory of the offence. But this was about to change. A new Article 65-3 of the Press Act created by the

⁵¹ Penal Code articles 131–35.

⁵² Penal Code, articles 225-2 and 432–7.

⁵³ Penal Code, article 223–13.

⁵⁴ This paragraph owes much to Laslier, 2024.

Law of March 9, 2004 adapting the justice system to developments in criminality⁵⁵ extended to one year the statute of limitations for offences of incitement to discrimination, hatred or violence on the grounds of the victim's belonging or not belonging to a particular ethnic group, nation, race or religion, to the denial of crimes against humanity and to racially motivated defamation and insults. Then, by more recent amendments, the one year time limit was applied to further offences: provocation, defamation and insult committed on the grounds of gender, sexual orientation or identity, or disability⁵⁶ and, in 2017⁵⁷, to these same offences when they were committed because of the victim's gender identity.

Legislators for some time favoured a method of increasing the quantum of punishment in the presence of behaviour constituting hate speech. To illustrate this point, we can refer to the general aggravating circumstances set out in articles 132-76 and 132-77 of the Penal Code. The purpose of these circumstances is to increase the custodial sentence incurred for an offence committed for reasons relating to the victim's actual or assumed belonging or not belonging to a particular race, ethnic group, nation or religion, or to his or her actual or assumed sex, sexual orientation or gender identity. Created in 2003,⁵⁸ these aggravating circumstances were subsequently generalized in 2017.⁵⁹ This generalization means that repression is systematically aggravated in the presence of discriminatory behaviour or expression. The legislator did not, however, include the disabled in the conditions that may provoke discriminatory motivation from the offender. This wasn't necessarily an omission: disability was probably not yet considered a cause for hatred.

1.7. Hate speech in a volatile jurisprudence

The judicial application of hate speech laws continues to fluctuate to this day. Two main trends coexist.⁶⁰ The first tends to condemn even expressions intended to provoke feelings of rejection, hostility and even hatred capable of violence,

55 Loi n° 2004-204 du 9 mars 2004 portant adaptation de la justice aux évolutions de la criminalité.

56 Loi n° 2014-56 du 27 janvier 2014 visant à harmoniser les délais de prescription des infractions prévues par la loi sur la liberté de la presse du 29 juillet 1881, commises en raison du sexe, de l'orientation ou de l'identité sexuelle ou du handicap.

57 Loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté.

58 Loi n° 2003-88 du 3 février 2003 visant à aggraver les peines punissant les infractions à caractère raciste, antisémite ou xenophobe.

59 Loi n° 2017-86 du 27 janvier 2017 relative à l'égalité et à la citoyenneté.

60 Hochmann, 2022, p. 4. The Supreme Court decisions cited here are also quoted by Hochmann in this article.

as stated in a 1976 Supreme Court ruling.⁶¹ In this sense, in 2017 the Supreme Court upheld the conviction of the mayor of a small town who had called the Roma a ‘nightmare’ and regretted that the ambulance had been called in time when a Gypsy caravan was set on fire.⁶² According to another interpretation, sanctions can only be imposed if the perpetrator has incited or encouraged hatred, violence or discrimination. If such incitement, even implicit, cannot be established, criminal liability is not established. In the classic example, the statement ‘Brutus is a traitor!’ is not punishable, but if we add: ‘He must therefore be killed’, then it is. This is what emerges from another relatively recent ruling by the Supreme Court. In the original case, the defendant was accused of inciting discrimination, hatred or violence through his tweets, the subject of which was mainly the changing ‘racial’ composition of the French national soccer team. However, the courts of first instance and of appeal found only one of the messages punishable, in which the author suggested that those who were ‘not French but on paper’ should be removed from the French national team. Finally, the Supreme Court ruled that this was a call for discrimination.⁶³ In a similar case, a group of friends, some of them off-duty police officers, while drinking, chanted Hitler and white supremacy and invoked death to the Jews. Convicted, they appealed to the Supreme Court, arguing that the appeal court had misinterpreted the Pleven Law, which requires incitement or provocation to hatred to be directed against a precisely identifiable person or group, and that they had merely expressed their political opinions, admittedly in a public place, but without addressing the public. However, the Supreme Court considered that Hitlerism, the ideology of white power, the call to reopen the gas chambers – all these elements delineated with sufficient precision the group of people whom the authors felt should be discriminated against, hated and subjected to violence.⁶⁴ At the same time, the same jury upheld the acquittal of the author who, in an article on the Rwandan genocide, had described the Tutsis as ‘the most mendacious race under heaven’.⁶⁵ Éric Zemmour, journalist turned presidential hopeful in the 2022 elections, regularly attacks immigrants, Muslims in

61 ‘...tending to arouse in the minds of readers feelings of hatred towards immigrant workers and as constituting calls for racial discrimination and even violence’. Cour de Cassation, Criminal Division, April 12, 1976, 74-92.515.

62 Cour de Cassation, February 1, 2017, 15-84.511.

63 Cour de Cassation, November 13, 2019, 18-85.371.

64 Cour de Cassation, March 28, 2017, 15-80.875. Hochmann cites this ruling with what we think is an erroneous conclusion, when he mentions it among the cases in which the courts, through their too narrow interpretation, reject the charge of incitement to hatred.

65 Cour de Cassation, November 8, 2011, 09-88.007.

particular. He has been tried several times for incitement to hatred under the Pleven Law, but never convicted. In an interview, Zemmour boasted that he was careful not to talk about religion or ethnic groups as a whole, so that his remarks could not be described as racist.⁶⁶ In 2021, Zemmour was acquitted by the Paris Court of Appeal of charges of hate speech. According to the prosecution, Zemmour wanted to incite hatred for speaking publicly about the invasion and colonization of France by Muslim immigrants. The court justified the acquittal on the grounds that Zemmour had not spoken of all immigrants or of all Muslims in general, but only of a group of them, a common set of ‘Muslim immigrants’.⁶⁷ The question arises as to why the cartoons of Mohammed in *Charlie Hebdo*⁶⁸ and other sometimes crude mockery of different religions, notably Islam and Christianity, do not fall under the norms prohibiting incitement to hatred. According to Hochmann, the answer to this question lies in the fact that the *Charlie Hebdo* cartoonists do not target a particular religion or its followers in general, but specific behaviours such as sectarianism, fundamentalism, etc.⁶⁹ In like manner, the Supreme Court more recently found that a verbal attack against a person as ‘Islamist’ is not discriminatory and cannot be qualified as hate speech because it does not denigrate a religion or a religious population but merely a specific political orientation.⁷⁰ In addition, the offence of blasphemy does not exist in French law. Moreover, the whole question may fall within the scope of what is sometimes referred to as the ‘right to humour’.

A recent decision of the Supreme Court is worth citing to illustrate the sometimes heated public debate. A controversial and militant antiracist activist, Taha Bouhafs was found guilty by a Paris Court of public insult on the grounds of origin, ethnicity, nation, race or religion under Articles 23, 29 and 33 of the Press Act after he called Linda Kebbab, a police officer and trade union delegate an ‘Arabe de service’, a ‘token Arab’. Bouhafs appealed to the Supreme Court on the grounds that both he and the opposite party share the same ethnic origin, a fact which in his view excludes any possible racist motive. Yet the Supreme Court upheld the verdict, reasoning that ‘the expression ‘token Arab’ presents [Ms. Kebbab] as a servile and complacent person, serving as an alibi and pretext, on

66 ‘J’avais dit le mot magique’ comment Eric Zemmour évite habilement les condamnations, Gala, 17 November 2021. https://www.gala.fr/l_actu/news_de_stars/il-sait-ou-se-situe-la-ligne-comment-eric-zemmour-evite-habilement-les-condamnations_479674

67 Cour d’appel de Paris, September 8, 2021, no. 20/05847.

68 In January 2015, a jihadist terrorist squad attacked the editorial office of French satirical magazine *Charlie Hebdo* in revenge for the publication of cartoons mocking the Prophet Mohammed, killing twelve and wounded eleven people.

69 Hochmann, 2022, p. 11.

70 Cour de cassation 14 mai 2024 Pourvoi n° 23-84.323.

account of her origin, for those who defend the police force denounced as violent and racist' and that this expression 'was in fact contemptuous of her, defined solely by her supposed origin and designated by an outrageous term, so that, constituting an insult, it exceeded the permissible limits of freedom of expression'.⁷¹ The judgment of the Supreme Court may go down as a landmark decision and have significant political impact. This time, namely, the legal argument was not between a party coming from the majority society versus and another representing a minority. Instead, two different visions within the same ethnic or cultural minority clashed: the offender viewed French social and political order as intrinsically racist and intolerant and insisted that anyone belonging to the same ethnic and cultural background as himself share his view. The Court now gave a boost to those with immigrant origin who have chosen the path of integration and loyalty to the Republic.

There are still some authors who are not entirely reconciled with the very concept of 'hate speech' let alone with its codification as an offence. Out of a handful of objections put forward by Brenaut, let me now choose two. The first regards the *exceptio veritatis* principle which is easily applicable to the classical case of insult and defamation under the Press Act but poses a challenge when they are motivated by racial or segregationist intentions, thus becoming 'hate speech'. Under the ICERD 'any doctrine of superiority based on racial differentiation is scientifically false...',⁷² an axiom the contrary of which cannot be proven in any trial. The second concern is the eventual clash between Article 10 and Article 17 of the European Convention of Human Rights. Article 10 safeguards free speech whereas Article 17 is meant to prevent the abuse thereof: 'no protection of the Convention for the enemies of the values of the Convention'. Yet the line between free speech and hate speech remains blurred and any hope to find objective criteria is likely to remain futile. At best, the defendant can try to claim that he has acted in good faith, without the intention of harm in the context of a debate of public interest or as a form of artistic expression (e.g. humour) and then call upon Article 10 to exonerate himself. Much is still left to case law and to the rather subjective assessment of the judge, each with his different convictions and sensitivities. So much so, that we may be faced with the 'freedom of expression *à la* Schrödinger': the same discourse can be both hate

71 December 19, 2023 Cour de Cassation n° 22-86.384 <https://www.courdecassation.fr/decision/6582bbc8747015f3f52007eb>

72 Preamble to the International Convention on the Elimination of All Forms of Racial Discrimination adopted 21 December 1965 by UN General Assembly Resolution 2106.

speech and part of a legitimate public debate until the judge ‘opens the box’ and discerns its content.⁷³

The maxim ‘no liberty for the enemies of liberty’, attributed to St. Just⁷⁴ can have grave legal consequences as in the case of Imam Mahjoubi whose expulsion was ordered by the French Minister of Interior after his heinous public remarks about the French tricolour and the Jewish people. He applied to the Paris Administrative Court to overturn the measure but the judge found that the comments made by the applicant were sufficiently serious to justify his expulsion from France, even though he had lived for a long time and had strong ties there.⁷⁵ In a similar case, another imam was condemned because an inflammatory sermon in which he included quotations from the Koran that incite the killing of Jews because of their ‘moral corruption’. The Supreme Court later confirmed the verdict ‘declaring the accused guilty of incitement to racial hatred, making it also clear that the issue at stake was not to assess the validity of a religious text, but the use that may have been made of it, its meaning and scope, in the context of preaching’.⁷⁶

Hervieu points out the decisiveness of case law in this regard. Again, how to distinguish between apology for terrorism and what could be part of a public debate? A rigid definition could be counterproductive: ‘an overly theoretical definition would, after all, either prevent any penal repression of comments exalting terrorist violence; or, on the contrary, it would further encroach on freedom of expression by fuelling self-censorship.’ Ultimately, nothing makes legal sense without a case-by-case analysis of the comments made: contexts, intention, the personality of the perpetrator are all to be assessed. In any case, the guidance provided by the ECHR in *Handyside v. the United Kingdom*⁷⁷ remains a key reference: freedom of expression applies also to ‘ideas that offend, shock or disturb’. It is worth noting that until 2014, the criminal offence ‘justification of terrorism’ was included in the Press Act after which it was transferred to the Penal Code. This implied the removal of a number of guarantees linked to press offences which used to take better account of freedom of expression. Creating new guarantees should be considered to avoid political instrumentalisation of criminal proceedings, the prohibition of any automatic summons by the police of persons reported for apology for terrorism until the public prosecutor or, better still,

⁷³ Brenaut, 2024.

⁷⁴ Ibid.

⁷⁵ Tribunal administratif de Paris N° 2404728/9 Ordonnance du 4 mars 2024 <https://rb.gy/wk6c60>

⁷⁶ Cour de cassation Pourvoi n° 22-87.200 paragraph 7. <https://www.courdecassation.fr/en/decision/6582bbc8747015f3f52007ea>

⁷⁷ *Handyside v. the United Kingdom* (Application no. 5493/72) 7 December 1976.

a judge has seen the file. There are concerns that judges are increasingly forced into the role of arbiter in political debates taken to court in the form of legal proceedings. In the aftermath of Hamas's terrorist attack on Israel on October 7, 2023, e.g., there has been a marked increase in the number of prosecutions for justification of terrorism.⁷⁸

2. Cyberbullying: sui generis offences vs. qualifying circumstances

2.1. *Digitalization of criminal offences*

Since 2003, the Penal Code carried a fine or even a prison sentence for anyone who would disturb the peace and quiet of others by making malicious telephone calls. Judicial practice extended this to text messages, until the legislator himself felt it necessary to update the norms so as to take account of the proliferation of new electronic devices of every kind. In 2014, it added 'repeated electronic messages' to the offence of telephone calling. The standard penalty is up to one year's imprisonment and a fine of up to 15,000 euros.⁷⁹ This could have given rise to a separate criminal offence: online harassment. But the legislation went in a different direction, as we shall see momentarily.

Before taking a look at the rules governing cyber bullying or online harassment, it's worth saying a few words about harassment in general. The French Penal Code defines three types of harassment:

- a) sexual harassment (*harcèlement sexuel*);⁸⁰
- b) moral harassment (*harcèlement moral*);⁸¹
- c) school harassment (*harcèlement scolaire*), as a specific kind of moral harassment.

However, one would look in vain for online harassment under this title of the Penal Code or anywhere else. This does not mean that the conduct in question goes unpunished. This subject has its own legislative evolution, which is probably far from over.

⁷⁸ Hervieu, 2024.

⁷⁹ Penal Code, art. 222-16.

⁸⁰ Penal Code 222-33, para 6°.

⁸¹ Penal Code art. 222-33-2-2, para 4°.

With the digital revolution, more and more offences can be committed via the Internet. French criminal law responds to this development in four main ways:⁸²

- a) Committing the offence online is specified in the law as *modus operandi*. Examples include identity theft, which also covers digital identity.⁸³
- b) The order of criminal liability is subjected to sector-specific rules: the regime of subsidiary liability for press offences committed by electronic means is modified in relation to that of the printed press.⁸⁴
- c) Committing the offence online or by means of the Internet is a special aggravating circumstance for certain forms of harassment (this is the most relevant to our subject, so we shall deal with it in more detail below).
- d) The case law of the French Supreme Court assesses the digital *modus operandi* and determines the consequences.⁸⁵

The Penal Code therefore considers the use of the Internet an aggravating circumstance for certain offences. These include rape, indecent assault, human trafficking, forced prostitution of a minor, receiving stolen goods. For these four offences, the penalty is more severe if the first contact between the perpetrator and the victim was established via the Internet.⁸⁶ In the case of child pornography, the online diffusion of contents entails a harsher punishment and the very acts of subscribing to or habitually consulting a website transmitting child pornography constitute an offence.⁸⁷

The situation is similar for sexual harassment and moral harassment. The current penal provisions on sexual harassment are the result of a 2018 amendment on combating sexual and gender-based violence.⁸⁸ The legislation was adopted following a comprehensive report on online violence against women published in early 2018 by the Commission for the Promotion of Equality between Women and Men set up under President François Hollande.⁸⁹ This report concluded that the perpetrators of such violence remain largely unpunished. The

⁸² Mesa, 2022, p. 125.

⁸³ Penal Code, art. 226-4-1.

⁸⁴ Audiovisual Communications Act article 93-3. For further details, see the section on Responsibility of service providers and institutions below.

⁸⁵ For example, according to the jurisprudence of the Supreme Court, it is not necessary for the author to have physically obtained the data medium, even partially, in order to establish data theft. Mesa, 2022, p. 125.

⁸⁶ Penal Code art. 222-24, 8°; 222-28, 6°; 225-4-2, 3°; 225-12-2, 2°; 225-7, 10°.

⁸⁷ Ibid. art. 227-23.

⁸⁸ Loi n° 2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes art. 11.

⁸⁹ HCE, 2017; Quemener, 2018.

report's starting point is to clarify two concepts: online violence against women (*violences faites aux femmes en ligne*) and virtual violence (*cyberviolences faites aux femmes*), preferring the former of the two formulas because it better expresses the fact that violence is real in terms of the harm caused, only the *modus operandi* or the 'place' in which the violence is committed is specific. The report then looks at two phenomena in particular. The first is a specific form of domestic violence online, where one of the parties (usually the man) exercises digital control or domination over the other: the perpetrator follows the other's every move in virtual or even real space, using various tracking devices (*cyber-contrôle dans le couple*). This is a latent but widespread behaviour, on which there are no precise statistics in France. The other particularly widespread form of harassment is the so-called digital raid (*raid numérique*). Typical victims are often female politicians or influencers who themselves defend women's rights or dignity. The report cites several concrete cases. In a particularly egregious instance, a youtubeuse who has gained notoriety for her investigation of street harassment received a shocking 40,000 messages, several of which included threats of murder or rape.. Penalizing this practice, however, posed a number of problems for legislators. The difficulty lay in the subjective behaviour of the perpetrators. One of the constituent elements of harassment is its repetitive nature. In this case, it takes the form of words or gestures with sexual or sexist connotations, which humiliate or degrade the victim, with the aim of placing him or her in a situation of fear, hostility or insult.⁹⁰ In the case of digital raid, the individual perpetrator does not necessarily repeat the act, but the victim is nevertheless subjected to a series of attacks. For the offence to be constituted, it is not even necessary for the perpetrators to agree to act in concert; it is enough for them to know that other people are also posting similar comments about the victim. The standard punishment is two years' imprisonment and a fine of 30,000 euros. In addition to the classic aggravating circumstances (offence committed against a person under the age of fifteen or a person subordinate to the offender or otherwise vulnerable, or in a group), the 2018 law added the offence committed online. If the aggravating circumstances are met, the penalty is increased to three years and 45,000 euros. Perpetrators of this type of group harassment are nevertheless difficult to prosecute. A circular letter from the Minister of Justice explaining the law asks prosecutors to take action against at least the instigators

90 'Sexual harassment is the repeated imposition on a person of sexual or sexist proposals or behaviors that either violate their dignity because of their degrading or humiliating nature, or create an intimidating, hostile or offensive situation.' Penal Code Art. 222-33.

or main perpetrators.⁹¹ The Penal Code extends the offence of digital raid not only to sexual harassment, but also to harassment in the workplace.⁹²

The Penal Code includes an offence similar to online harassment among the offences of invasion of privacy, when the offender discloses conversations, words or images of sexual content of another person without his or her consent. It should be noted that, although it is nowadays on the Internet that insults of this kind nowadays typically happen, the legislator makes no distinction between offline and online modes.⁹³

2.2. Moral harassment at work, at home, at school... anywhere

The structure of the section of the Penal Code on moral harassment is somewhat peculiar. It reflects an evolution that appears historical rather than dogmatic which manifests itself in a series of responses the legislator gave to the emerging new forms and modalities of abusive conduct – just as I attempted to describe them in the previous paragraph. The basic definition in Article 222-33-2 reveals the origin of the provision whose objective is to penalize that kind of conduct which can make one's life in the workplace unbearable 'by repeated comments or behaviour with the purpose or effect of causing a deterioration in working conditions likely to infringe on their rights and dignity, alter their physical or mental health or compromise their professional future.' The maximum punishment for this is two years in prison. This offence has not been 'digitalized': there is no reference to committing it online. Then the text goes on to apply this, *mutatis mutandis*, to domestic abuse committed against a current or former spouse, civil partner (*partenaire lié par un pacte civil de solidarité*) or common-law partner.⁹⁴ Here the definition becomes already more articulate, though. The basic punishment is three years in prison and a considerable fine (€45.000). This article envisages some aggravating circumstances including various degrees of incapacity for work as an effect or the presence of a minor. If the harassment results in an attempted or completed suicide, the punishment increases to ten years in prison. No digital *modus operandi* is mentioned here, either.

The next article (222-33-2-2) carries the most comprehensive and general definition of harassment. It retains and completes the constituent elements of

91 Circulaire du 3 septembre 2018 relative à la présentation de la loi n°2018-703 du 3 août 2018 renforçant la lutte contre les violences sexuelles et sexistes. Available at: <https://www.legifrance.gouv.fr/circulaire/id/44010>.

92 Penal Code, article 222-33-2-2.

93 Penal Code, article 226-2-1.

94 Article 222-33-2-1 of the Criminal Code.

moral harassment used by the two previous articles but does not restrict the group of potential victims to any category of persons or a particular context. The two new constituent elements were added in the context of combating digital raids, as mentioned above. Therefore, the offence is also constituted when the abusive ‘comments or behaviour are inflicted on the same victim by several persons, in concert or at the instigation of one of them, even though each of these persons has not acted repeatedly’, or when the offence is committed against ‘the same victim, successively, by several persons who, even if not in concert’, are aware that their comments or behaviours constitute a repetition. The basic punishment is up to two years in prison with a substantial fine. The statutory aggravating circumstances are:

- a) Incapacity to work for more than eight days as a result;
- b) The victim is a minor;
- c) The victim is a person whose particular vulnerability, due to age, illness, infirmity, physical or mental deficiency or pregnancy, is apparent or known to the perpetrator;
- d) If the offence is committed by the use of an online public communication service or through a digital or electronic medium;
- e) The offence was committed against an elected official (*titulaire d’un mandat électif*);
- f) A minor was present and witnessed the offence.

The punishment is increased to three years in prison and to €45,000 if at least two of these conditions are met. So here we are in front of the ‘digitalization’ of harassment. (With no ‘suicide clause’ is attached, though.)

In 2022, the French Parliament passed a law on school harassment (School Harassment Act, SHA)⁹⁵, introducing it as an offence by adding a new article (222-33-2-3) to the section on moral harassment of the Penal Code. It refers back to the constituent elements of the previous article. However, here the victim can only be a pupil or student, while the perpetrator can either be a pupil or a teacher. To the previously mentioned aggravating circumstances, the lawmaker added suicide with the same wording as in the case of domestic abuse. By contrast, the digital *modus operandi*, i.e. cyberbullying at school is missing.

The SHA amended several provisions of the Code of Education. The latter already included a specific title on health protection in schools, including a separate chapter on abuse prevention.⁹⁶ It now requires all teachers to undergo spe-

⁹⁵ Loi n° 2022-299 du 2 mars 2022 visant à combattre le harcèlement scolaire.

⁹⁶ Code of Education art. L.542-1 to L.542-4.

cific training in youth protection, including a course on sexual offences against minors and their consequences. School bullying as an offence as well as the obligation to take more specific measures against it, have been introduced into the Code of Education. As noted above, the Code of Education nowhere uses the term ‘cyberbullying’, but in literature and legal practice it is considered implicit in the concept of school harassment.⁹⁷ The same applies to the question of whether disciplinary or more severe sanctions are attached to offences committed outside school walls.⁹⁸ A case in point is an appeal brought by a father whose son had been expelled from a high school after sending indecent videos to a female fellow student. The father asked the administrative court to annul the measure on the grounds that his son committed the offence outside the school, at a party, and therefore could not have breached school discipline. But the administrative court ruled that the act was inseparable from the offender’s status as a high school student and from the condition that the offender and his victim were students at the same school. The behaviour therefore caused an inevitable and serious disruption to the life of the school. A ministerial circular note pointed out that the proliferation of social media is increasingly blurring the boundaries between students’ lives inside and outside school.⁹⁹

The SHA integrated the overall prohibition of harassment, i.e. the ‘right to a harassment-free school environment’, into the general provisions of the Code of Education. The long, detailed definition, as if wanting to leave nothing to chance (or to the judge?), says: ‘No pupil or student may be subjected to harassment resulting from comments or behaviour within the school establishment or in the context of school or university life, which have the purpose or effect of undermining his or her dignity, altering his or her physical or mental health or compromising his or her academic progress. These acts may constitute the offence of school harassment as provided for in Article 222-33-2-3 of the Penal Code’.¹⁰⁰

Another group of provisions of the SHA reinforces the material and procedural instruments of criminal law to combat harassment in schools and universities. Amending the Penal Code, it establishes the criminal offence of school harassment, as described above. Under the Code of Criminal Procedure (CCP),

⁹⁷ Article L.511-1. The *Commentaire Dalloz* is available by subscription in the publisher’s online library: <https://www.dalloz.fr/documentation/Document?id=EDUC003000>

⁹⁸ *Ibid.*

⁹⁹ Lettre de la direction des affaires juridiques du ministère de l’éducation nationale et du ministère de l’enseignement supérieur, de la recherche et de l’innovation LIJ N°202 – May 2018. Available at: https://www.education.gouv.fr/lettre-information/lettre-information-juridique/PDF/LIJ_2018_202_mai.pdf

¹⁰⁰ Code of Education art. L.111-6.

the investigating or prosecuting authority may seize the computer of the suspect/accused and the data stored on it in the case of an Internet offence.¹⁰¹

As there is a specific Penal Code¹⁰² for Minors in France, the law has also included certain provisions on bullying at school. E.g. a secondary sanction may be imposed on the bully, such as an obligation to complete an internship or practical training.¹⁰³

3. Right to a harassment-free environment

The potentially tragic consequences of cyberbullying are well understood by lawmakers, law enforcement agencies and the public. Numerous articles in the French press explain that these consequences can go as far as suicide.¹⁰⁴

A Ministry of Education circular in 2013 was the first to take stock of possible ways of preventing and dealing with the problem. It identifies them mainly in terms of raising awareness and maintaining a climate of trust; e.g., by making students aware that cyberbullying is unacceptable, and that it can lead to disciplinary or even penal consequences. Channels must be set up in all educational establishments to enable victims to come forward and seek help quickly, easily and confidentially. The circular reminds school principles of the toolbox at their disposal, including, in the most serious cases, the possibility of filing a criminal complaint.¹⁰⁵

The French ombudsman (Défenseur des droits) addressed the issue of harassment at school and online in his 2021 communication and report. The report points out that in recent years, political decision-makers have grown aware of the seriousness of the situation and, as a result, society, children and students now have more tools at their disposal to protect themselves: anti-harassment counsellors in all schools, free helplines and forums, action plans and teaching materials. Nevertheless, the problem persists, with the number of cases stagnating at a high level. The reasons for that include the persistence of an attitude that trivializes verbal and physical violence, to some extent regarding it as part of

101 SHA art. 12, which amends several provisions of the CCP.

102 Code de la justice pénale des mineurs.

103 SHA Art. 15.

104 The subject is examined in depth in an international study by Leiden University researchers published in 2014: van Geel-Vedder-Tanilon, 2014.

105 Circulaire n° 2013-187 du 26-11-2013 in Le bulletin officiel de l'éducation nationale, de la jeunesse et des sports n° 44 du 28 novembre 2013. Available at: https://www.education.gouv.fr/bo/13/Hebdo44/MENE1329057C.htm?cid_bo=75290

life; in other cases, the educational establishment deems it sufficient to transfer either the bully or the bullied to another school.¹⁰⁶

In February 2024, the findings of the first comprehensive national survey of the phenomenon were published, based on anonymous questionnaires filled in by a representative number of pupils and high school students. The victimization index is defined as the number of repeated attacks suffered. The survey shows that 3% of elementary school pupils have experienced eight or more assaults; 5% of middle school students have experienced five or more assaults; 3% of high school students have experienced five or more assaults.¹⁰⁷

The Code of Education, among its aforementioned provisions on a bullying-free school environment, requires primary, secondary and higher education facilities, both public and private, to take appropriate measures to combat the phenomenon, with an emphasis on prevention. It is the responsibility of the teaching community to create an atmosphere in which it is easy to detect harassment, provide effective response, counsel victims, wrongdoers and witnesses alike, and direct them to institutions that can help them. The Code of Education also makes it compulsory for pupils, students and parents to organize at least one annual awareness-raising session on the dangers of harassment, particularly digital.¹⁰⁸ The Code of Education now entrusts an important role to the health, citizenship and environment education committees of public secondary schools whose mission is to work with parents and other players outside the school to combat truancy and other harmful phenomena, using social mediation and artistic and cultural education in particular. Since March 2022, the law has therefore included the fight against bullying among the missions of this committee.¹⁰⁹ The scope of the Code of Education extends not only to public, but also to private education.¹¹⁰ The SHA not only amended the Code of Education, but also made awareness-raising and training mandatory in all sectors, so that all professionals likely to be confronted with school bullying are aware of its existence and are able to protect victims and manage their traumas. Doctors, nurses, social workers, judges, teachers and other educational staff, sports, cultural and recreational staff, police and gendarmerie receive training in the

106 Avis du Défenseur des droits n°21-10, Paris, le 12 juillet 2021. Available at: https://juridique.defenseurdesdroits.fr/doc_num.php?explnum_id=20852, as well as Rapport 2021. Santé mentale des enfants: le droit au bien-être Available at: https://juridique.defenseurdesdroits.fr/doc_num.php?explnum_id=21061

107 Premiers résultats statistiques de l'Enquête harcèlement 2023. Available at: <https://t.ly/VbHm7>

108 Code of Education Art. L.111-6.

109 Code of Education art. L.421-8.

110 Ibid. art. L.442-2, L.452-3-1.

prevention, identification of and assistance to victims, witnesses and offenders. Such training should be offered to all professionals working in educational establishments.¹¹¹ Guidelines on how to prevent and confront harassment in schools have to be defined in the school's statutes or curriculum.¹¹² It is also the responsibility of the school doctor to check, during routine examinations, whether the pupil or student shows signs of harassment suffered.¹¹³

However, the Code of Education not only deals with the issue of harassment in terms of health and mental health risks or criminal law aspects, but also introduces it into the school curriculum. The law dedicates a long article to defining the ethical and civic knowledge to be taught. The intention is to help students become 'responsible and free citizens who acquire a critical sense and the ability to act reflectively, including in their use of the Internet and online public communication'.¹¹⁴ The text in italics shows that, although the Code of Education does not use the term cyberbullying or online harassment, the legislator had not forgotten about it. Other subjects covered by ethics and citizenship include, e.g., the rights and equal opportunities of disabled persons, a preference for fair trade, free from child labour and the promotion of voluntary and community activities. The SHA also provides that students must be informed about who they can turn to, apart from the authorities, if they become victims of harassment. The law addresses not only victims but also potential offenders and seeks to prevent them from turning into actual ones.

The provisions of the Code of Education described so far apply mainly to secondary schools. However, the scope of the law also extends to universities. Book VIII of the Code, dedicated to 'university life', provides for the creation in universities of an environment conducive not only to academic, but also social advancement of students, including, where appropriate, social assistance. A favourable environment now includes the fight against harassment.¹¹⁵

'High school ambassadors against harassment' (*ambassadeurs lycéens contre le harcèlement*) have been appointed. This initiative dates back to 2015. There are currently around 5,000 'ambassadors'. The idea is simple: students will volunteer to monitor and detect harassment in their own environment, among their peers, to intervene if necessary, or to raise awareness in their communities by showing them examples of acceptance and cultural coexistence. In particular, they are responsible for ensuring the quality of personal relationships within

111 SHA art. 5.

112 SHA art. 5.

113 Code of Education art. L.542-2.

114 *Ibid.*, L312-15.

115 Act L.822-1.

the community, comforting and supporting victims of harassment, and taking action against bullies. The Education Ministry's website contains very detailed recommendations on how the 'ambassadors' should carry out their duties. They can organize, i. a., meetings with pupils about bullying, informing fellow students about how to recognize the phenomenon, who to contact, possible remedies, etc.¹¹⁶ One of the obvious advantages of student ambassadors is that young people are less ashamed to talk with each other about their experience than with adults, let alone the authorities. The institution of student ambassadors seemed also justified by some discouraging statistics. 5.6% of students reported having been victims of it. Seven percent of those regularly experience some form of cyberbullying.¹¹⁷

In a recent effort to keep up with the rapidly changing digital and digitalized social environment, the French Parliament in June 2023 passed a bill regulating commercial influence and combating the abuses of influencers on social networks.¹¹⁸ It amends, i. a., the Education Act setting the ambitious goal of educating and training people to the responsible use of digital tools and resources. It imposes this task on schools and educational establishments across a wide range of sectors, including, e.g., agriculture, health care, social services, etc. The education should cover the rights and duties associated with the use of the Internet, social media, also with regard to the protection of privacy and respect for intellectual property, freedom of opinion and the dignity of the human person and the image of women, as well as data protection. Lawmakers wanted to promote the 'development of critical thinking', contribute 'to the fight against the dissemination of hateful content online, to raising awareness of commercial manipulation and the risks of online scams, and to learning about digital citizenship'. Special training should be provided to teach users how to detect and report illegal content. The training also includes raising awareness of the prohibition of harassment committed in the digital space, ways of digital self-defence and the penal sanctions the wrongdoing entails. In sum, it promotes 'digital sobriety' (*sobriété numérique*) — a succinct expression, this. The latest amendment, in May 2024 extended risk awareness to AI. At the end of primary and

116 Available: <https://www.education.gouv.fr/devenir-ambassadeur-au-lycee-323018#edugouv-summary-item-4>

117 For less recent but more detailed research findings, see Blaya, 2018. For more details on student ambassadors, see <https://www.education.gouv.fr/non-au-harcelement/le-dispositif-des-ambassadeurs-non-au-harcelement-323021>

118 LOI n° 2023-451 du 9 juin 2023 visant à encadrer l'influence commerciale et à lutter contre les dérives des influenceurs sur les réseaux sociaux.

lower secondary school, they receive a certificate of successful completion of the training.¹¹⁹

4. Liability: service providers and institutions in a ‘cascade’

4.1. From printed press to social media: editorial responsibility sublimating

The question is how to enforce the authorities’ action against online crime, cyberbullying and hate speech. To overview French legislation in this regard is not devoid of challenge. In addition to the Press Act, other laws contain relevant provisions. Freedom of opinion and expression, on the one hand, and the prevention of hate speech, on the other, are two mutually contradicting desiderata. Between them the lawmaker has to perform a balancing act on a tightrope that is stretched each time at a new height over a new abyss. The relentless development of new media, devices, apps, platforms and whatnot, combined with new, sometimes eccentric forms of art, views, etc. also requires the ceaseless updating of relevant legislation. However, the French lawmaker is responding not only by amending the Press Act, but also by adopting new *sui generis* laws which, in turn, also update the fundamental source of the law, the very same Press Act.

The Press Act lays down the rules governing liability for offences committed through the press. According to these rules, the director of the publishing house (*directeur de publications*), the editor-in-chief or the co-editor-in-chief are considered primarily liable. If there are none, or if they are exempt from liability for whatever reason, the author (*auteur*), printer, distributor, poster (*afficheur*), etc. are liable, in that order (*responsabilités en cascade*).¹²⁰

The Press Act did not prove adequate in the face of the spreading of the new electronic audio-visual media. Under the 1982 Audio-visual Communications Act, where the offence is committed by electronic means, the publisher or co-publisher responsible for the publication is deemed to be the offender, failing which the author or, failing that, the creator of the entry is liable in the first instance. However, the author is liable as an accomplice in any event. The publisher is not liable for content uploaded to the site by users, provided that he

¹¹⁹ Code of Education art. L312-9.

¹²⁰ Press Act, art. 42.

had the offending content removed as soon as it was discovered and brought to his knowledge.¹²¹

The aforementioned Léotard Law on freedom of communication is an important piece of legislation. It originally covered the traditional audio-visual media, i.e. radio and television. In 2020, it was supplemented by a specific Title IV for online platforms, including provisions to combat online hate content. This defines in great detail the duty of cooperation that platform operators must have with ARCOM. ARCOM considers the risks specific to each platform and may adopt different guidelines and recommendations for each operator. These generally include the obligation to communicate service parameters and principles, taking into account restrictions on personal data. ARCOM can also require the operator to provide data. ARCOM can also impose a fine of up to six per cent of the previous year's turnover or a maximum of 20 million euros for failure to comply with the obligation to cooperate.¹²² Besides pecuniary sanctions, ARCOM has a toolbox at its disposal:

- a) Suspension of the publication, broadcasting or distribution of the service(s) of a program category, part of the program or one or more advertising sequences for one month or more;
- b) Reduction of the duration of the authorization or license agreement by up to one year;
- c) Withdrawal of the authorization or unilateral termination of the license agreement.¹²³

4.2. Addressing constitutional limits to immediate removal of illegal content

In the age of the printed press, the spread of illicit content was slow. Newspapers would be published once a day at best with only nationwide circulation. Things are very different in cyberspace: irreparable damage can be done with the speed of light among an audience as wide as the globe. How can even the most rapid justice system keep up? A civil process can take years while a quick harm would call for a quick fix. The Avia Law, also mentioned above, would have obliged operators of online platforms and search engines to remove blatantly illegal content, such as hate speech, racist or religiously defamatory content, within twenty-four hours of one or more complaints. In the case of terrorist content or child pornography, the deadline was set at one hour. However,

121 Loi n° 82-652 du 29 juillet 1982 sur la communication audiovisuelle Art. 93-3.

122 Léotard Law art. 62.

123 <https://www.arcom.fr/alertez-nous/comment-larcom-reagit-vos-alertes>

in June 2020,¹²⁴ the Constitutional Council ruled that most of these provisions were unconstitutional. On the one hand, it confirmed the legislator's power to punish abuses of freedom of expression when such expressions are contrary to public order or the rights of third parties. More than ever, it specified that the dissemination of pornographic images of minors constitutes a particularly serious infringement of this freedom, as does incitement to commit terrorist offences or the glorification of such offences. On the other hand, the Constitutional Council rejected the obligations imposed by the Avia Law on operators for several reasons. In the case of terrorist content or child pornography, the Constitutional Council considered that the illegality could only be established by a court and that the time limit of one hour was not sufficient for a court to formulate and notify its decision. This restriction on freedom of expression therefore failed to meet the combined requirements of proportionality and necessity. The Constitutional Council noted the risk that platforms and content providers might become overly zealous to remove all potentially controversial content, including what is deemed risky but may be legal, thus fostering a climate of self-censorship.

The French legal system continues to struggle with the question of how to eliminate vicious content from the Internet as rapidly as possible without getting caught in the net of the Constitutional Council again. As we saw above, the Separatism Act made an effort to overcome the constitutional hurdle, creating the possibility for the administrative authority to request the removal of illicit contents of the following kinds:

- a) contents that incite or condone (apologie) terrorist acts as defined by the Penal Code¹²⁵;
- b) images or representations of minors as defined in the same code¹²⁶.

The process of removal is the following, on the basis of the current text of the LCEN.¹²⁷

The administrative authority (ARCOM, typically) may request the editor, host or anyone who is in charge of the content and its online diffusion¹²⁸ to take action. (For the purposes of this paragraph, I shall refer to this first category as 'host'.) The authority simultaneously informs the pertinent ISP. The deadline of removal is 24 hours. If the deadline is not met, the administrative authority may

124 Décision n° 2020-801 DC du 18 juin 2020.

125 Penal Code art. 421-2-5.

126 Ibid. art. 227-23.

127 In particular, art. 6 to 6-5.

128 No matter if the service is provided free of charge.

notify the ISP to immediately prevent access to the problematic address. A third option is to notify the search engine or the directory of electronic addresses so that it may stop referencing the web site. Consciously false notifications with the purpose of having content removed is punished with remarkable severity: one year in prison and 15.000 euros in penalty. Even more serious punishments are involved for the hosts that fail to observe their obligations under the procedure above or to provide the information necessary for cooperation with the authorities and the public for the sake of suppressing illicit on-line contents. It seems clear to me that the legislator wanted to promote online transparency without which cyberspace would be doomed to become the place of highly dangerous activities.

The injunction to remove content or make it inaccessible can be challenged by the service providers in an administrative court within 48 hours; the court has seventy-two hours to decide about the legality of the removal order. Its decision can be appealed. The court of appeal has one month to decide.¹²⁹

The procedure just presented here applies to the justification of terrorism and online child abuse.

In May 2024, the latest major revision of the pertinent legislation took place when Parliament adopted Law no. 2024-449 to secure and regulate the digital space (SREN Law).¹³⁰ The SREN Law updates extensively a series of pertinent legislation, the LCEN and the Penal Code in particular.¹³¹ The text also strengthens penalties for people convicted of online hate, cyber-harassment or other serious offences (child pornography, pimping, etc.). The judge will be able to impose an additional penalty of suspension or ‘banishment’ from social networks for six months (or even a year in the event of a repeat offence). If the social network fails to block the suspended account, it will be liable to a fine of 75,000 euros.¹³² The online publication of hypertrucages or ‘deep fakes’ will be punished more severely. Schoolchildren are to be made aware of the dangers of AI-generated contents.¹³³ At the start of the school year, parents will be informed of the dangers of early and unsupervised exposure of children to screens and the risks

129 LCEN Art. 6-1-5. Among these provisions there are some that constitute a more rigorous regime with regard to explicitly terrorist content under Regulation (EU) 2021/784 of 29 April 2021 on addressing the dissemination of terrorist content online.

130 Loi n° 2024-449 du 21 mai 2024 visant à sécuriser et à réguler l’espace numérique.

131 See also <https://rb.gy/d3gclu>

132 SREN art. 16.

133 Ibid. art. 21., Penal Code art. 226-8-1.

associated with the Internet. A ‘digital citizen’s reserve’, as a thematic part of the ‘civic reserve’¹³⁴ will be set up.¹³⁵

4.3. Collaboration of the platforms with users and authorities

The Separatism Act adapted the liability rules to take account of the constitutional objections and amended the LCEN accordingly. It maintained the scope of application of the Avia Law, platforms that transmit, distribute or reference online content produced by third parties. A platform or content provider falls within the scope of these provisions when the number of connections on French territory reaches a certain number, defined by decree, whether the service provider is established or registered in France or abroad. We note that the provision has been drafted to target the major platforms, which also happen to be the main vehicles of hate content: Facebook, X (formerly known as Twitter), Instagram, YouTube, etc.¹³⁶

The law requires the subjects to employ sufficient human and technological resources to ensure that they have the capacity to remove illegal content. The legislator wanted to prevent operators from leaving everything to algorithms. They are obliged to implement procedures and proportionate human and technological resources enabling them to collaborate with judicial and administrative authorities. Such collaboration covers the following elements:

- a) The platforms inform the authorities of the actions they have taken in response to injunctions issued by these authorities;
- b) They acknowledge receipt of requests from these authorities for the communication of data in their possession enabling the identification of users who have put the illicit content online and inform the authorities of the action taken;
- c) They temporarily store the content they have removed or made inaccessible, in order to make it available to law enforcement agencies.¹³⁷

Platforms have to designate a natural person as a contact point for communicating with the authorities through a single channel.

¹³⁴ This national ‘pool’ brings together offers of volunteer work from citizens aged 16 and over, wishing to contribute to missions proposed by associations, local authorities and public administrations. <https://www.jeunes.gouv.fr/la-reserve-civique-277>

¹³⁵ SREN art. 23.

¹³⁶ Bigot, p. 22.

¹³⁷ LCEN art. 6-4 para 2.

Platforms have to display their conditions of use, with special regard to the prohibition of illicit content. The information also should describe their moderation system designed to detect, identify and deal with illicit content, the human or automated resources employed for this purpose, as well as the measures they may take with regard to users who have put such content online, as well as the internal and legal remedies available to such users. In sum, legislation obliges the platforms to take action against its own users, if necessary, working with the authorities eventually even for their prosecution.¹³⁸ The law introduces a specific provision for the protection of minors. When a user under the age of fifteen subscribes to a service on the platform, the person with parental responsibility must be warned that if the minor publishes or shares hateful content, the parent will be held responsible.¹³⁹

The Separatism Act tackled the so-called mirror sites (*site miroir*), known to be used both to deflect hacker attacks and to republish content declared illegal on sites that look identical to the original. The removal of illegal content does not require a new procedure or court ruling, but can be requested on the basis of the previous judgment. A list of providers who have been convicted and ordered to remove access to hate content is also to be made public. In order to financially stifle rogue sites, the law obliges advertisers to indicate on their website whether they do business with a 'blacklisted' site, following the 'name and shame' principle, already known from the fight against pornography or tax evasion.¹⁴⁰

4.4. Compromises in the current liability regime

The current provisions of the LCEN regarding this subject are as follows. On the one hand, they exempt the service provider or the medium from civil liability if it was ignorant of the manifestly unlawful nature of the content it has published or stored on the Internet, provided it makes it inaccessible immediately after notified or becoming aware of it. A similar exemption applies to criminal liability. On the other hand, the lawmaker wanted to protect lawful contents from groundless or, indeed, abusive challenges: so the same provision also incriminates complaints made in bad faith with the sole aim of obtaining removal or inaccessibility. Notification or complaint concerning unlawful content may not be anonymous but must include basic information (name, address, etc.) about the person (natural person or a legal entity, including a public authority) who is filing it; a description of the contested content, its nature, its exact location

¹³⁸ Ibid. art. 6-4, para 3. Bigot, 2021, p. 24.

¹³⁹ Ibid. art. 6-5. Bigot, 2021, p. 25.

¹⁴⁰ Ibid. art. 6-3. Bigot, 2021, pp. 27-29.

on the Internet and the content of the contestation.¹⁴¹ In addition, the LCEN provides an explicit general exemption for service providers from the obligation to constantly monitor whether unlawful content is being put online. So, as we have just said, platforms and hosts only have to act on notification, and not by their own initiative. Contents liable to prosecution are listed: denial or trivialization (banalisation) of crimes against humanity; incitement to commit terrorist attacks or the exaltation of such acts; incitement to hatred based on race, sex, sexual orientation or identity, disability; child pornography; incitement to violence, in particular gender-based or gender-related violence; and offences against human dignity. This section is closely linked to the aforementioned Chapter IV of the Press Code on press offences, and to the relevant provisions of the Penal Code, in that it stipulates that the service provider must cooperate in the removal of such content, and is also subject to a reporting obligation if such content is discovered.¹⁴²

In the case of online harassment, the cascade of responsibility is different, and so is the procedure to be followed.¹⁴³ Unlike hate speech, where the primary local responsibility lies with the publisher or, in the case of online media, the content provider standing in for him (albeit with the restriction that he can claim ignorance of the illegal content), the primary responsibility for harassment on the Internet lies with its perpetrator. However, service providers who transmit the content in question (*intermédiaires techniques*) are also liable in this order:

- a) social media platforms (e.g. Facebook, X, games, blogs, file-sharing sites, etc.) that host or share content produced by a third party (*hébergeur*), or
- b) the Internet service provider.

However, the penal, administrative and civil liability of intermediaries and file sharers is limited and conditioned on notification and awareness. They can only be held liable if they, although knowing of the harassing content, have failed to remove it promptly. The Constitutional Council noted the risk that platforms and content providers would become eager to remove all potentially controversial content, including that which is deemed risky but may be legal, thus giving rise to self-censorship. Therefore, they are not expected to check the legality of countless messages, posts, images, etc., that are being shared. The victim can

141 Ibid. art. 6. Para I-2-5. Bigot, 2021, p. 19.

142 LCEN art. 6 para I-7. Bigot, 2021, *ibid*.

143 A summary of liability rules and the procedure to be followed is available on the French public service portal: <https://www.service-public.fr/particuliers/vosdroits/F32075>. See also art. 6 of the LCEN and art. 93-3 of the Audiovisual Communications Act.

request the removal of the content, firstly from its author and, if this fails, from the platform, forum, etc. This request has not to be necessarily accommodated by the platform applying French laws but applying its own rules instead. Each major social media, file-sharing or other platform has its own rules on the formalities and conditions for requesting removal or blocking. If this procedure does not yield the expected result, the victim can refer the matter to the authorities, in accordance with French law. In urgent cases, an injunction (référé) can be requested from the court to stop the harassment immediately. If criminal liability is involved, the victim can also take such action. They can also file a complaint with the police or gendarmerie. An offence can be reported to the police even if the offender is unknown, as the identity of the perpetrator remains often hidden in cyberspace – in such case, the service provider is obliged to cooperate in identifying the abuser.

4.5. Competence and jurisdiction

Since social media is essentially a global network, the question of jurisdiction arises in the event of infringement. Content published on the Internet can be contested before a French court if the content in question

- a) is in France, available in French, or
- b) is intended for the French public, or
- c) affects the interests of a person living in France.

This is the case even when the author does not stay in France, or if the content is not on a French website. It may be a personal blog, a video or a social media post. Content can be prosecuted even when it is not accessible to all Internet users. For example, it may only be accessible to certain ‘friends’ on a particular platform.

In addition, for those who should find a police procedure too formal and rigid, it is also possible to lodge a complaint on an online platform, called Pharos, created for this purpose with the idea that anyone can be either victim or witness of cybercrime on social media. Pharos will, in turn, report the case to the police or the gendarmerie.¹⁴⁴

144 Available: <https://www.internet-signalement.gouv.fr/PharosS1/>

Summary

Freedom of speech and expression is a core principle of the French constitutional order. This freedom should be, however, accompanied by responsibility since the Declaration of the Rights of Man and of the Citizen. Restrictions on freedom of expression for reasons of public interest and overriding private interests may therefore be in line with the Constitution. But it remains a challenge for legislators, courts and other authorities alike to strike a delicate and ever changing balance. The most relevant legislative source for hate speech is the Freedom of the Press Act, passed in 1881 and still in force today, amended several times, which from the outset has contained penal sanctions for ‘classic’ press offences like defamation and insult. This may be regarded as a French particularity, given that in several other European countries penal sanctions cannot be imposed but in the penal code. The digital revolution and the proliferation of new online media has led to the proliferation of the expressions of hate. To combat racism and other forms of incitement against groups and communities has become a necessity in order to preserve social peace. The legislator has sought to respond to changing social demands by introducing new laws amending and updating the old ones. ‘Traditional’ offences like insult, defamation or pimping are being ‘digitalized’, which means they are easier to commit online. Harassment or bullying is another obvious example. There are other forms of illicit conduct that have been born with and on the Internet like ‘doxing’ and ‘digital raid’. Yet French lawmakers seem hesitant to define and introduce separate, *sui generis* cybercrimes. They prefer a different avenue, where the use of the Internet as *modus operandi* becomes a special or aggravating circumstance. The development of legislation generally takes place through comprehensive legislative amendments, in large interdisciplinary steps, reforming from time to time several areas of law and the legal norms that define them. In the case of hate speech, radio and television were included first, and then the Internet as the media that can be abused for the propagation of hate speech. In recent times, the French lawmaker has been compelled to intervene with increasing speed and frequency by adopting new provisions within the Press Act, the Penal Code, the Code of Education and in other sectors affected by expressions of hate such as telecommunication and the workplace also in an effort to boost confidence in the digital economy. Basically, the French legislature tackled the problem of racial hate speech and cyberbullying earlier than other European countries, but its responses in a rapidly changing social and political context cannot be considered definitive.

Liability rested with the newspaper editor in olden days for he was supposed to read all he would publish. In the age of online social media, the same cannot be

expected of any service provider. Instead of one single liable subject, we are now in the presence of a ‘cascade of responsibilities’ where liability largely hinges on the notification of the illicit content to the service or platform provider. The lawmaker’s attempt to impose the duty on Internet service providers and social media platforms to make hateful content immediately and almost automatically inaccessible has failed the constitutional test. The Constitutional Council was reluctant to approve solutions that may encroach on freedom of expression without robust judicial control. This leaves only the normal legal route and cooperation with service providers, whether voluntary, encouraged or forced. The internal policies of the major platforms generally prohibit illicit expressions themselves, so it is possible to ask them to remove those. Some non-legislative tools to prevent and combat cyberbullying are also available, mainly in the area of bullying in schools. The latter is characterized by a high level of government awareness among teachers, students and parents, and by strengthening students’ capacity for self-organization and peer empowerment by introducing the institution of student ‘ambassadors’ to combat cyberbullying.

All in all, France can boast an extensive and sophisticated set of legislative tools to combat a culture of hate, but a restless social and political environment, combined with the exaltation of freedom of expression as the most cherished constitutional achievement, leaves much of the balancing act to the courts.

Bibliography

- Bigot, C. (2021) 'Les discours de haine et les contenus illicites en ligne', *Revue Française de Droit Administratif (RFDA)*, 37(5), pp. 835–844
- Blaya, C. (2018) 'Cyberbullying in France' in Baldry, A. C., Blaya, C., Farrington, D. P. (eds.) *International Perspectives on Cyberbullying: Prevalence, Risk Factors and Interventions*. 1st edition. Cham: Palgrave Macmillan
- Brahim, R. (2020) 'La législation antiraciste française, support d'un racisme structurel', *Communications*, 2020/2, pp. 237–250
- Brenaut, M. (2024) Quels motifs d'exonération de leur responsabilité pénale pour les prévenus en matière de discours de haine? *Revue des droits et libertés fondamentaux RDLF 2024 chron. n°12* [Online]. Available: <https://revuedlf.com/droit-penal/quels-motifs-dexoneration-de-leur-responsabilite-penale-pour-les-prevenus-en-matiere-de-discours-de-haine/>
- Gala (2021) 'J'avais dit le mot magique' comment Eric Zemmour évite habilement les condamnations, 17 November 2021. [Online]. Available: https://www.gala.fr/l_actu/news_de_stars/il-sait-ou-se-situe-la-ligne-comment-eric-zemmour-evite-habilement-les-condamnations_479674
- HCE (Haut Conseil à l'Égalité entre les femmes et les hommes) (2018) En finir avec l'impunité des violences faites aux femmes en ligne: une urgence pour les victimes [Online]. Available: https://www.haut-conseil-egalite.gouv.fr/IMG/pdf/hce_rapport_violences_faites_aux_femmes_en_ligne_2018_02_07.pdf
- Hervieu, N. 'Mieux vaut toujours prendre le risque de la liberté d'expression que de son bâillonnement', *Le Nouvel Obs*, Publié le 30 avril 2024 [Online]. Available: <https://www.nouvelobs.com/justice/20240430.OBS87793/mieux-vaut-toujours-prendre-le-risque-de-la-liberte-d-expression-que-de-son-baillonnement.html>
- Hochmann, T. (2022) 'Du lustre après dix lustres: la loi de 1972 contre le racisme a cinquante ans', *Revue des droits de l'homme*, 2022/21. DOI: 10.4000/revdh.14356
- Hochmann, T. (2024) 'Les discours de Haine, le droit pénal et la cour européenne des droits de l'homme', *Revue des droits et libertés fondamentaux, RDLF 2024 chron. n°05* [Online]. Available: <https://revuedlf.com/cedh/les-discours-de-haine-le-droit-penal-et-la-cour-europeenne-des-droits-de-lhomme/>
- Kondorosi, F. (2015) 'Paradigm shifts in the international legal assessment of freedom of expression', *ACTA Humana*, 2015/2, pp. 81–96.
- Laslier, P-F. (2024) 'La sanction pénale des discours de haine: quelles difficultés répressives?' Appartient au dossier: "Discours de haine et droit pénal" *RDLF*

- 2024 chron. n°14 [Online]. Available: <https://revuedlf.com/droit-penal/la-sanction-penale-des-discours-de-haine-quelles-difficultes-repressives/>
- Letteron, R. (2023) *Libertés publiques* (Kindle Edition)
- Ministère de l'éducation nationale, Ministère de l'enseignement supérieur, de la recherche et de l'innovation (2018), Lettre de la direction des affaires juridiques du Ministère de l'éducation nationale et du Ministère de l'enseignement supérieur, de la recherche et de l'innovation LIJ N°202 – May 2018. [Online]. Available: https://www.education.gouv.fr/lettre-information/lettre-information-juridique/PDF/LIJ_2018_202_mai.pdf
- Mesa, R. (2022) 'Le droit pénal général à l'épreuve de l'infraction digitalisée', *Recueil Dalloz*, 2022/3. p. 125.
- Quemener, M. (2018) 'Cyberharcèlement: quelles évolutions législatives?' *Lamyline Actualités du droit*, 7 December 2018 [Online]. Available: <https://www.actualitesdudroit.fr/browse/penal/droit-penal-special/18194/cyberharcèlement-quelles-evolutions-legislatives>
- Van Geel, M., Vedder, P., Tanilon, J. (2014) 'Relationship Between Peer Victimization, Cyberbullying, and Suicide in Children and Adolescents: A Meta-analysis', *JAMA Pediatr*, 168(5), pp. 435–442. doi:10.1001/jamapediatrics.2013.4143
- Villard, M. (2001) 'La liberté d'expression dans l'Histoire' in *Bulletin de l'Académie du Var*. Toulon: Académie du Var, pp. 137-148.

XIX. HATE SPEECH AND CYBERBULLYING IN ITALY

ÁLMOS UNGVÁRI

Introduction

The Constitution of the Italian Republic¹ guarantees anyone the right to freely express their thoughts in speech, writing, or any other form of communication.² This freedom is not absolute, there are several explicit and implicit limitations to the right to freedom of expression in the Italian legal system.³ However – unlike for example the Fundamental Law of Hungary – the Constitution of Italy does not contain any explicit provisions on this fundamental right that could be considered as a prohibition of hate speech. But over time, several laws have been adopted which penalize various forms of discrimination and hate speech.⁴

1. Hate Speech Regulation

The origin of the Italian regulation of discrimination and hate speech is Section XII of the Transitional and Final Provisions of the Constitution of Italy.⁵ This provision forbids the reorganization of fascist parties under any form. For a period of not more than five years from the implementation of the Constitution

1 Costituzione della Repubblica Italiana (hereinafter: Constitution of Italy).

2 Constitution of Italy Article 21 (1); Egresi, 2013, pp. 185–187.

3 Falletta, 2020, p. 149.

4 Abbondante, 2017, pp. 56–58.

5 Basile, 2019, p. 2.

of Italy, the right to vote and eligibility for the leaders responsible for the Fascist regime were temporarily limited.⁶ This prohibition was expanded by the so-called Act Scelba,⁷ which also punishes the organization and propaganda of fascist initiatives with fines and imprisonment.⁸

The first stage of the regulation of hate speech in Italy can be defined⁹ as Act No. 654 of 1975 on the proclamation of the International Convention on the Elimination of All Forms of Racial Discrimination, adopted in New York on 21 December 1965 (hereinafter: Act 1975/654).¹⁰ In addition to the proclamation of the international convention, Act 1975/654. provided for imprisonment for the dissemination of ideas of racial superiority or hatred, incitement to national, ethnic or racial discrimination or violence against persons belonging to such groups, or the commission of violent acts. The establishment of organizations and associations with such aims, and participation in them and their activities, was also prohibited.¹¹ Act 1975/654. was amended by Act No. 122 of 1993 on urgent measures on racial, ethnic and religious discrimination,¹² also known as the Act Mancino. The modified law also penalized incitement to hatred and violence on religious grounds.¹³ It also prohibited, as a preventive measure, the display of symbols expressing discrimination or incitement to hatred on racial, ethnic or religious grounds or belonging to organizations established for such purposes.¹⁴ Thus the Act Mancino broadened the scope of discriminatory acts that are punishable. According to Italian jurisprudence, while with the adoption of Act 1975/654, the legislator aimed to give priority to the protection of public order, the main value to be protected in Act Mancino was human dignity.¹⁵ The

6 Constitution of Italy Transitional and Final Provisions Section XII.

7 Act No. 645 of 1952 on Implementing the Transitional and Final Provisions Section XII (1) of the Constitution of Italy (*Legge 20 giugno 1952, n. 645: Norme di attuazione della XII disposizione transitoria e finale (comma primo) della Costituzione*).

8 See e. g. Pulitanò, 2019, 12–17. pp.; Basile, 2019, pp. 2–3.

9 Marsocci, 2021, p. 220.; Leoni, 2016, p. 12.

10 *Legge 13 ottobre 1975, n. 654: Ratifica ed esecuzione della convenzione internazionale sull'eliminazione di tutte le forme di discriminazione razziale, aperta alla firma a New York il 7 marzo 1966* (hereinafter: Act 1975/654).

11 Act 1975/654. 3. §.

12 *Decreto-Legge 26 aprile 1993, n. 122: Misure urgenti in materia di discriminazione razziale, etnica e religiosa* (hereinafter: Act Mancino). Converted with amendments by the following act: *Legge 25 giugno 1993, n. 205: Conversione in legge, con modificazioni, del decreto-legge 26 aprile 1993, n. 122, recante misure urgenti in materia di discriminazione razziale, etnica e religiosa*.

13 Act Mancino 1. §.

14 Act Mancino 2. §.

15 Leoni, 2016, 13. p. On Act Mancino see e. g. Castellani, 2021, 7–8. pp.; Marsocci, 2021, 220. p.; Basile, 2019, 8. p.; Falletta, 2020, p. 150.

Act No. 115 of 2016¹⁶ also amended the Act 1975/654. This amendment provides for a more severe penalty, as a kind of qualified case, if the propaganda or incitement is aimed at denying or diminishing the significance of the Holocaust or relates to genocide, crimes against humanity or war crimes.¹⁷

As a final step in the legal development of the prohibition of hate speech, the provisions adopted until then were incorporated into the Italian Criminal Code¹⁸ in 2018.¹⁹ Thus, the Italian Criminal Code includes²⁰ propaganda and incitement to commit a crime based on racial, ethnic and religious discrimination²¹ among the crimes against equality.²² Under the legislation in force, anyone who disseminates ideas based on superiority, incites racial or ethnic hatred, incites discrimination on racial, ethnic, national or religious grounds or commits such a criminal offence is punishable by imprisonment or a fine. It is important to note that this is a subsidiary criminal offence, meaning that the offender can only be punished under these provisions if a more serious criminal offence has not been committed.²³ The establishment of any organisation, association, movement or group which aims to discriminate or incite violence on racial, ethnic, national or religious grounds is prohibited. Anyone who participates in or assists in such activities shall be liable to imprisonment. More serious offences are committed by those who promote or direct such organizations, associations, movements and groups.²⁴ As described above, the Italian Criminal Code specifically names and punishes hate speech related to Holocaust denial with imprisonment from two to six years.²⁵ In addition, the Italian Criminal Code provides, as a general rule, that the penalty for criminal offences punishable by imprisonment for a term other than life imprisonment is increased by half if the criminal offence is committed with discriminatory

16 Legge 16 giugno 2016, n. 115: Modifica all'articolo 3 della legge 13 ottobre 1975, n. 654, in materia di contrasto e repressione dei crimini di genocidio, crimini contro l'umanità e crimini di guerra, come definiti dagli articoli 6, 7 e 8 dello statuto della Corte penale internazionale.

17 See e. g. Pulitanò, 2015, pp. 325–332.; D'Amico, Fiano, 2021, pp. 130–131.; Rosato, 2016, pp. 280–312.

18 Codice Penale (hereinafter: Italian Criminal Code).

19 Decreto Legislativo 1 marzo 2018, n. 21: Disposizioni di attuazione del principio di delega della riserva di codice nella materia penale a norma dell'articolo 1, comma 85, lettera q), della legge 23 giugno 2017, n. 103.

20 Vallini, 2020, pp. 45–46.; D'Amico, Fiano, 2021, pp. 128–130.

21 Propaganda e istigazione a delinquere per motivi di discriminazione razziale etnica e religiosa.

22 Delitti contro l'eguaglianza.

23 Italian Criminal Code 604-bis § (1).

24 Italian Criminal Code 604-bis § (2).

25 Italian Criminal Code 604-bis § (3).

motives or in order to promote the activities of organizations, associations, movements or groups formed for the purpose of ethnic, national, racial or religious hatred or for the promotion of such hatred.²⁶

In recent years, there have been several calls to extend the criminal offence of hate speech to discrimination and incitement to hatred based on gender identity or sexual orientation. Recently, the Chamber of Deputies voted in favor of draft legislation, known as the Act Zan,²⁷ which would have amended the 604-bis and 604-ter paragraphs of the Italian Criminal Code. As a result of which, the criminal offence could have been committed in relation to gender identity and sexual orientation.²⁸ However, the crime was not amended because the Senate did not pass the amendment.

The major challenge for hate speech jurisprudence is to find the point at which an expression exceeds the constitutional freedom of expression.²⁹ In this regard, the Italian Constitutional Court³⁰ has stated in several previous decisions³¹ – prior to the codification of hate speech – that freedom of expression is not always and, in all circumstances, a fundamental right that must be unconditionally protected. It may be restricted for the purpose of enforcing other constitutional rights. According to the principles of necessity and proportionality.³² According to the case law, there must be a direct link between the speech and the action triggered. It must be intended to influence public opinion and change the mindset of the audience.³³ The latter was ruled by the Supreme Court of Cassation³⁴ in a case where the accused wrote about ritual murders committed by Jews on a website, naming Jews as satanic enemies of God and the people against whom a holy war must be waged.³⁵ There is also anti-Semitic hate speech in the condemnation of a vegetarian animal rights activist professor

26 Italian Criminal Code 604-ter § (1).

27 Disegno di legge Zan, also known as DDL Zan, from the name of the first signatory of the proposal, Member of Parliament Alessandro Zan.

28 See: Occhipinti, 2020.

29 Santerini, 2021, p. 144.

30 Corte Costituzionale.

31 For example: Decision of the Italian Constitutional Court No. 19 of 1962, Decision of the Italian Constitutional Court No. 25. of 1965, Decision of the Italian Constitutional Court No. 87. of 1966, Decision of the Italian Constitutional Court No. 100. of 1966, Decision of the Italian Constitutional Court No. 20. of 1974, Decision of the Italian Constitutional Court No. 15. of 1973, Decision of the Italian Constitutional Court No. 16. of 1973, Decision of the Italian Constitutional Court No. 133. of 1973, Decision of the Italian Constitutional Court No. 86. of 1974.

32 D'Amico, Fiano, 2021, p. 32.

33 Basile, 2019, 4. p.; D'Amico, Fiano, 2021, p. 141.

34 Suprema Corte di Cassazione.

35 Judgment of the Supreme Court of Cassation No. 37581. of 2008.

at the University of Cagliari. In his study, the slaughter of animals according to Jewish rituals was criticized, saying that it is the natural right of animals to avoid suffering. In his argument, he relativized the Holocaust, stating that Jews could not expect respect for their lives.³⁶ A much-cited Supreme Court of Cassation ruling on a racist speech by a city councilor at a city assembly is also worth mentioning. In this case, the acquittal was overturned because of the defendant's public political role and the high profile of the speech.³⁷ However, there are also a number of cases where offensive speech is protected by the court under freedom of expression. The case of the writer Oriana Fallaci is a good example. In one of her writings, she used insulting terms against Islam and its followers, calling them enemies of the Western world, without distinguishing between moderate and extremist Muslims. At the preliminary hearing, the judge ruled that it was an argument against the mass immigration of Muslims to Europe. Thus, the author had not exceeded the limits of freedom of expression. Therefore, no charges were brought in the case.³⁸ The case law on the Act Scelba, which criminalizes fascist initiatives, is very poor. The condemnations³⁹ mostly concern the use, display or publication of typically fascist symbols, such as the Roman salute or the Celtic cross, or the various commemorations.⁴⁰ There is no practice in relation to the criminal offence of hate speech constituting Holocaust denial.⁴¹ It is noteworthy that during the coronavirus pandemic, there was a significant increase in hate speech.⁴² Such as anti-Semitic opinions or offensive comments related to the attitude towards the management of the pandemic. A good example of the latter is the case of Senator Liliana Segre, whose picture documenting the administration of the coronavirus vaccine triggered a huge wave of hatred on social media.

Also, in Italy the phenomenon of online hate speech is a new emerging problem and needs to be solved as soon as possible. With the development of info communication technologies, the emergence of the Internet and in particular social media, new platforms are available for the crimes concerned. And these platforms can not only transmit but also intensify hate speech, increasing its efficiency.⁴³ The continuous evolution of technology poses a

36 Judgment of the Supreme Court of Cassation No. 20508. of 2012.

37 Judgment of the Supreme Court of Cassation No. 47894. of 2012.

38 Basile, 2019, p. 5.

39 For example: Judgment of the Supreme Court of Cassation No. 8108. 2018, Judgment of the Supreme Court of Cassation No. 11038. 2017.

40 Pulitanò, 2019, pp. 13–14.

41 Basile, 2019, pp. 10–11.

42 See e. g. Santerini, 2021, p. 155.; D'Amico, Fiano, 2021, pp. 134–135.

43 Castellani, 2021, pp. 11–12.; Ziccardi, 2021, p. 167.; Santerini, 2021, p. 143.

major challenge in terms of creating legislation that responds to the challenge of constant change. Several legislative proposals⁴⁴ have been drafted in recent years. And the Italian Charter of Rights on the Internet⁴⁵ was also adopted, which stipulates the principles on the use of the internet, the protection of human dignity, the prohibition of discrimination and freedom of expression. However, we do not find an adequate legal framework for online hate speech in the Italian legal system.⁴⁶ With regard to the liability of internet service providers for the publication or transmission of hate speech, only the Directive on electronic commerce⁴⁷ and the legislative decree⁴⁸ transposing it into national law are of some relevance.⁴⁹ The Directive on electronic commerce stipulates the liability of intermediary service providers with regard to mere conduit, caching as well as hosting.⁵⁰ For example the provider, upon obtaining actual knowledge of illegal activity or information and awareness of facts or circumstances from which the illegal activity or information is apparent, acts expeditiously to remove or to disable access to the information.⁵¹ However the Directive on electronic commerce also stipulates the absence of general obligation of the providers to monitor the information which they transmit or store and to actively seek facts or circumstances indicating illegal activity.⁵²

So, there is no real national regulation. Thus, the academic discourse from time to time raises the issue of rethinking and regulating the responsibility of the offender and the Internet service providers in relation to hate speech

44 For example: Amendments to the Criminal Code and other provisions to combat incitement to hatred and discrimination in 2018 [Modifiche al codice penale e altre disposizioni in materia di contrasto dell'istigazione all'odio e alla discriminazione (hate speech)]; Measures to counter the phenomenon of incitement to hatred on the web in 2019 (Misure per il contrasto del fenomeno dell'istigazione all'odio sul web); or the draft law on measures to prevent and combat the spread of hate speech on the internet, in 2021, which was similar to the German legislation (NetzDG) in its content and the way it combats online hate speech. See: D'Amico, Fiano, 2021, pp. 136–137.

45 Carta Italiana dei Diritti in Internet. See: Leoni, 2016, p. 15.

46 Di Tano, 2017, p. 114.

47 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 (hereinafter: Directive on electronic commerce)

48 Decreto Legislativo 9 aprile 2003, n. 70: Attuazione della direttiva 2000/31/CE relativa a taluni aspetti giuridici dei servizi della società dell'informazione nel mercato interno, con particolare riferimento al commercio elettronico. (hereinafter: Legislative Decree 2003/70.)

49 Nardi, 2019, p. 275.; Castellani, 2021, pp. 17–22.; Di Tano, 2017, pp. 119–120.

50 Directive on electronic commerce Article 12–15.; Legislative Decree 2003/70. 14–17. §.

51 Directive on electronic commerce Article 14.; Legislative Decree 2003/70. 16. §.

52 Directive on electronic commerce Article 15.; Legislative Decree 2003/70. 17. §.

offences.⁵³ The responsibility of the Internet service providers is a particularly interesting issue, because also in Italy there are cases in which profiles or pages have been deleted or made inaccessible by a social media outlet that has deemed their activities discriminatory or hateful. A good example is the recent case of the Italian neo-fascist political movement Casapound, whose page and many of its members' profiles were deleted from Facebook and Instagram. The case has led to a lively public debate, as in many other countries, about whether private companies that do not exercise public authority can restrict freedom of expression through decisions such as this one. Whether these companies can quasi-censor their users in line with their own community standards and rules.⁵⁴ In the case, the Tribunal of Rome⁵⁵ ruled that Facebook was obliged to operate in accordance with constitutional principles, but its decision violated the principle of pluralism. So, the Tribunal of Rome ordered the social network to reinstate the deleted account of the political party.⁵⁶ However, the correctness of the decision was questioned.⁵⁷ As in another case, Tribunal of Siena⁵⁸ ruled that the relationship between social platform operators and users is strictly private. In doing so, the Facebook's right to deactivate pages and profiles that engage in hate speech activities violating the community standards was recognized.⁵⁹ However, the Supreme Court has stated⁶⁰ that the hosting provider is liable in cases where the unlawful content was not removed immediately. The hosting provider is also liable if it continued to publish the unlawful content even though it knew of the illegality or should have been aware of it with reasonable care. Similarly, the hosting provider is liable if it has the opportunity to take the necessary action in the knowledge that it should have done so but fails to do so.

As regards the institutions, the Observatory for Security Against Acts of Discrimination⁶¹ and the National Office Against Racial Discrimination⁶² are worth mentioning. The former is an interforce agency (Italian National Police and Carabinieri Corps) established in 2010 and set up within the Public Security Department – Central Directorate of Criminal Police. It provides qualified

⁵³ See e. g. Castellani, 2021, p. 16.

⁵⁴ See more on the topic: Falletta, 2020, pp. 150–155.

⁵⁵ Tribunale di Roma.

⁵⁶ Venanzoni, 2019.; Manna, 2020.

⁵⁷ Falletta, 2020, p. 158.

⁵⁸ Tribunale di Siena.

⁵⁹ Decision of Tribunal of Siena of 19. January 2020. See: Falletta, 2020, p. 158.

⁶⁰ Decision of the Supreme Court No. 7708. of 2019.

⁶¹ Osservatorio per la Sicurezza contro gli Atti Discriminatori.

⁶² Ufficio Nazionale Antidiscriminazioni Razziali.

support to victims of discrimination offences (hate crimes). The latter was created by the Legislative Decree⁶³ No. 215 of 2003. on implementing Directive 2000/43/EC⁶⁴ in order to monitor the effective application of the means of protection against racial or ethnic discrimination. These are the two bodies most likely to receive reports and complaints about discriminatory acts in Italy. Both bodies receive the various complaints and, if necessary, inform the police. They also liaise with victims and protection services. They assist in the procedures and monitor the progress of the case. The Senate's special committee responsible for combating intolerance, racism, anti-Semitism and incitement to hatred and violence is also worth mentioning. This committee's activities include for example the removal of such content from the Internet. In addition, several associations and rights organizations play an important role in the fight against acts of hate speech.

The lack of a legal framework, but also many other aspects raise many issues in the field of hate speech, but the solution to these is not only the transformation and supplementation of the legal environment. Of course, it would be a priority to clearly define the liability of the users and providers of social networks for illegal conduct, or the minimum address range required to commit an infringement, in order to curb online hate speech.⁶⁵ However, while appropriate sanctions can act as a deterrent, the best way to prevent hate speech in the long term is to create an environment that does not tolerate it, and education is the most important tool in this regard.⁶⁶

2. Regulation of Cyberbullying

The phenomenon of bullying (*bullismo* in Italian) and cyberbullying (*cyberbullismo* in Italian) is also a serious problem in Italy, requiring public action in many areas. Thanks mainly to the development of technology, the daily use of electronic devices and the Internet, but most of all to the emergence of social media.⁶⁷

63 Decreto Legislativo 9 luglio 2003, n. 215: Attuazione della direttiva 2000/43/CE per la parità di trattamento tra le persone indipendentemente dalla razza e dall'origine etnica.

64 Council Directive 2000/43/EC of 29 June 2000 implementing the principle of equal treatment between persons irrespective of racial or ethnic origin.

65 Di Tano, 2017, p. 114.; Castellani, 2021, p. 11.

66 Di Tano, 2017, pp. 121–122.

67 Fierimonte, 2022.; Focaroli, 2020.; Motta, 2020a.; Grandi, 2017, 41–42. pp.; Sorrentino, Baldry, Cacace, 2018.

The Ministry of Education first addressed the issue of bullying in a 2007 directive,⁶⁸ setting out measures and general guidelines at national level to prevent and combat it successfully. The Directive defines bullying, referring to a commonly used term in international literature, as a continuous or persistent physical or verbal act that is intended to cause harm or injury to others. This interaction – which may include, for example, malicious gossip, the spreading of slander, or isolation from peers – does not merely affect one person, but by its very nature involves entire groups.⁶⁹ The phenomenon of cyberbullying is already present in this document but is even more prominent in subsequent ministerial directives with similar content (adopted in 2015,⁷⁰ 2017⁷¹ and 2021⁷²). These are essentially to ensure the continued operation of measures already underway, such as the regional centers set up by the 2007 Directive. What they all have in common is that the prevention and combating of bullying is mainly seen in the context of education, i.e. information and awareness-raising is essential.⁷³ The Ministry of Education's Safer Internet-Generazioni Connesse project, which raised awareness of the Internet and new media, is worth mentioning.⁷⁴ Mention should also be made of the self-regulatory code⁷⁵ adopted by the Ministry of Development in 2014, in which some operators and content providers of social networking services have committed to implement their own easily accessible and applicable rapid response mechanism to report activities that may constitute cyberbullying and remove harmful content. From all these measures and initiatives, the political will to take decisive action at state level against bullying and cyberbullying is evident.

The case of a fourteen-year-old girl who committed suicide in Novara, following videos posted on social media, has received national media coverage and generated a lot of publicity.⁷⁶ As a result of these and similar increasingly

68 Ministerial Directive No. 16 of 5 February 2007: General guidelines and nationwide actions to prevent and combat bullying (*Direttiva Ministeriale n. 16 del 5 febbraio 2007: Linee di indirizzo generali ed azioni a livello nazionale per la prevenzione e la lotta al bullismo*).

69 Russo, 2022.

70 Guidelines for actions to prevent and combat bullying and cyberbullying (*Linee di orientamento per azioni di prevenzione e di contrasto al bullismo e al cyberbullismo*).

71 Guidelines for preventing and combating cyberbullying (*Linee di orientamento per la prevenzione e il contrasto del cyberbullismo*).

72 Guidelines for preventing and combating cyberbullying (*Linee di orientamento per la prevenzione e il contrasto del cyberbullismo*).

73 Berlingò, 2018, pp. 1–3.; Liberali, 2015, pp. 20–22.

74 Bocchini, Montanari, 2018, pp. 349–350.

75 Self-regulatory code for preventing and combating cyberbullying (*Codice di autoregolamentazione per la prevenzione e il contrasto del cyberbullismo*)

76 Eremita, 2018, pp. 2–3.

frequent cases, the legislator has also recognized the need to protect young people as fully as possible at the legislative level,⁷⁷ and it is therefore justified to regulate the rules for combating bullying and cyberbullying at the legislative level. There have been a number of bills highlighting the importance of prevention and monitoring of this type of behavior.⁷⁸ These measures mainly consisted of the removal and inaccessibility of data that constituted offensive behavior. At institutional level, the creation of technical councils to coordinate the necessary measures and draw up an action plan, the setting up of monitoring centers and the creation of a network of schools to play a key role in victim support and awareness-raising were also considered appropriate. However, the need to involve experts and the role of the ministry in raising awareness of the use of the Internet were also mentioned in some of the draft laws.⁷⁹

Finally, after a long parliamentary debate⁸⁰ and several amendments, the Act No. 71. of 2017 on the provisions for the protection of minors to prevent and combat the phenomenon of cyberbullying⁸¹ was adopted⁸² in May 2017. The declared aim of this act was to combat all forms of cyberbullying, mainly through preventive actions, awareness-raising strategies, protection and education of minors concerned and the involvement of educational institutions. However,

77 See: Donati, 2019, pp. 63–65.

78 See e. g. Bill No. 2408. of 2014 on provisions to protect minors and prevent and combat bullying, including cyberbullying (Disposizioni a tutela dei minori per la prevenzione e il contrasto del bullismo, anche informatico); Bill No. 2435. of 2014 on provisions to prevent and combat bullying, including cyberbullying (Disposizioni per la prevenzione e il contrasto del bullismo, anche informatico); Bill No. 2534. of 2014 on the establishment of a permanent observatory against bullying, discrimination and violence (Istituzione di un Osservatorio permanente contro il bullismo, anche informativo, le discriminazioni e la violenza); Bill No. 1311. of 2014 on provisions for preventing and combating bullying and cyberbullying and the proper use of the Internet to protect minors (Disposizioni per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo e per la corretta utilizzazione della rete internet a tutela dei minori); Bill No. 2391. of 2010 on provisions on preventing and combating bullying in all its manifestations (Disposizioni in materia di prevenzione e di contrasto al fenomeno del bullismo in tutte le sue manifestazioni); Bill No. 1621. of 2014 on provisions for preventing and combating bullying and cyberbullying and the proper use of the Internet to protect minors (Disposizioni per la prevenzione e il contrasto del fenomeno del bullismo e del cyberbullismo e per la corretta utilizzazione della rete internet a tutela dei minori); Bill No. 1986. of 2014 on provisions for preventing and combating bullying and cyberbullying (Disposizioni per la prevenzione e il contrasto del bullismo e del bullismo informatico).

79 Liberali, 2015, pp. 22–25.

80 Eremita, 2018, p. 3.; Focaroli, 2020.

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

82 For more on the adoption of the law, see: Bocchini, Montanari, 2018, pp. 351–354.

the recently adopted Act No. 70 of 2024 on provisions and delegation of authority to the Government on the prevention and combat of bullying and cyberbullying (hereinafter: Act No. 70. of 2024)⁸³ has, among other things, extended the scope of the law to include the category of bullying.⁸⁴ Consequently, its title has also been changed to reflect this amendment: Act No. 71. of 2017 on the provisions for the protection of minors to prevent and combat the phenomenon of bullying and cyberbullying (hereinafter: Act No. 71. of 2017).⁸⁵ The Act No. 71. of 2017 now has the objective of combating all forms of bullying and cyberbullying.⁸⁶ It can still be stated that by educating and raising the awareness of the at-risk age group, the Act No. 71. of 2017 focuses on prevention and deterrence of offences instead of punishment.⁸⁷

Although the criminal law character was also stronger in other proposals and earlier drafts of the adopted law,⁸⁸ in the end, the Act No. 71. of 2017 did not include new criminal offence.⁸⁹ The measures provided by the act for victims of cyberbullying are also aimed more at remedying the harmful situation, their retaliatory nature is less relevant, and the legislator's intention to avoid criminal prosecution is evident. The most important innovation in the act is the definition of cyberbullying in the interpretative provisions. For the purposes of the Act No. 71. of 2017, cyberbullying is defined as electronic pressure, aggression, harassment, extortion, insult, defamation, slander, identity theft, alteration and manipulation, or unlawful processing of personal data, committed against minors. But it is also cyberbullying to disseminate online content about a minor's family member – or family members – with the intent and primary purpose of attacking the minor.⁹⁰ The legal definition of cyberbullying is not easy to define, as it can take many different forms and can be carried out through many different types of behavior. It may be noted that the Italian legislator did not actually undertake to do so either, but rather provided a very broad, heterogeneous list of conduct that could constitute cyberbullying. This heterogeneity also means, however, that the interpretative provision

83 *Legge 17 maggio 2024, n. 70: Disposizioni e delega al Governo in materia di prevenzione e contrasto del bullismo e del cyberbullismo* (hereinafter: Act No. 70. of 2024).

84 For more on Act No. 70. of 2024, see: Giordano, 2024.; Biffa, 2024.

85 *Legge 29 maggio 2017, n. 71: Disposizioni a tutela dei minori per la prevenzione e il contrasto dei fenomeni del bullismo e del cyberbullismo* (hereinafter: Act No. 71. of 2017).

86 Act No. 71. of 2017 l. § (1).

87 Benedetti, 2021, p. 170.; Bocchini, Montanari, 2018, p. 349.; Racca, 2018.; Ricotta, 2017.; Senor, 2017, p. 175.

88 Bocchini, Montanari, 2018, pp. 353–354.; Liberali, 2015, p. 24.

89 Colangelo, 2017, pp. 399–400.; Giordano, 2019.; Martorana, Sichi, 2021.

90 Act No. 71. of 2017 l. § (2).

treats acts of a different nature and with different perceptions together. Some conduct, such as harassment, defamation or unlawful data processing, is a criminal offence, while others are not. For this reason, some have considered the definition of cyberbullying too broad and criticised it. In addition, many also criticized the fact that, when drafting the definition of cyberbullying under Act No. 71. of 2017, the legislator ignored the internationally accepted sociological and criminological concepts and characteristics of the phenomenon, in particular the repetitive nature of the behavior causing harm.⁹¹

Also, the legislator's original decision not to include the concept of bullying in the adopted act, although it was included in some proposals and in the earlier stages of the legislative process, was widely disputed. According to some opinions, the legislator's decision was justified because the specificity of cyberbullying can cause serious harm in a loose temporal and spatial context, without physical contact and direct contact. Given the greater delimitation of bullying and the consequently less serious nature of its consequences, it was therefore acceptable to regulate the two categories in separate legislation.⁹² Others, however, considered the omission of offline bullying from the Act No. 71. of 2017 to be a serious mistake because of the close, inseparable relationship between the two concepts.⁹³ The main problem, however, is that with this omission there was still no legal definition of bullying.⁹⁴ However, the issue of regulation was so much on the agenda that since June 2020, two bills introducing the category of bullying into the Act No. 71. of 2017 have been before the Senate. Both drafts would declare the fight against bullying not only in cyberspace but also in 'traditional' bullying as the aim of Act No. 71. of 2017, and would include a definition of bullying in the interpretative provisions. However, the level of detail of the definition shows a difference between the two drafts. One draft⁹⁵ would add bullying to the current definition of cyberbullying, making

91 Benedetti, 2021, pp. 167–168; Bocchini, Montanari, 2018, pp. 354–356; Colangelo, 2017, p. 399; Motta, 2020; Rospi, 2017, pp. 465–466; Senor, 2017, pp. 175–176; Eremita, 2018, pp. 6–7.

92 Benedetti, 2021, pp. 168–169; Motta, 2020a.

93 Rospi, 2017, p. 474.

94 Motta, 2020b.

95 Bill No. 1690. on amendments to the Criminal Code Act No. 71. of 2017 and Royal Decree Law No. 1404 of 20 July 201934 converted with amendments, by Act No. 835 of 27 May 1935 on preventing and combating the phenomenon of bullying and re-educational measures for minors (*Modifiche al codice penale, alla legge 29 maggio 2017, n. 71, e al regio decreto-legge 20 luglio 1934, n. 1404, convertito, con modificazioni, dalla legge 27 maggio 1935, n. 835, in materia di prevenzione e contrasto del fenomeno del bullismo e di misure rieducative dei minori*).

the same conduct an actionable offence. However, the other draft⁹⁶ would specify in a separate paragraph that, for the purposes of the Act, bullying is aggression or harassment committed repeatedly against one or more minors by a person or a group of persons, with the purpose of causing distress or fear or isolating or excluding the victim. It also includes physical or psychological violence and pressure, incitement to suicide or self-harm, threats, blackmail, insults, and mockery, whether based on language, ethnicity, religion, gender, sexual orientation, physical appearance, disability or other personal or social characteristics. This proposal would therefore constitute a separate but similar concept in relation to the conduct listed.⁹⁷ Following the enactment of the Act No. 70. of 2024, the latter solution has been implemented. A new paragraph in the initial section of the Act No. 71. of 2017 stipulates that bullying means repeated aggression or harassment, by an individual person or group of persons, against a minor or a group of minors, suitable to provoke feelings of anxiety, fear, isolation or marginalization, through harassing acts or behavior, physical or psychological pressure or violence, incitement to suicide or self-harm, threats or blackmail, theft or damage, insult or mockery.⁹⁸

In addition the Government is delegated by the Act No. 70. of 2024 to adopt legislative decrees within 12 month in order to prevent and counteract the phenomena of bullying and cyberbullying. It is imperative that these legislative decrees guarantee, inter alia, the following: the strengthening of the service for the assistance of victims of bullying and cyberbullying through the public number “Child Emergency 114”; the biennial survey of the National Institute of Statistics on the phenomena of bullying and cyberbullying every; the initiative in relation to the implementation of awareness and preventive campaigns pertaining to the prudent utilisation of the Internet and its associated risks.⁹⁹

It is worth noting that several regions have adopted regional laws to combat all forms of bullying and cyberbullying. Including for example the regions of

96 Bill No. 1743. on amendments to Act No. 71. of 2017 and other provisions to combat the phenomenon of bullying and cyberbullying (*Modifiche alla legge 29 maggio 2017, n. 71, e altre disposizioni per il contrasto dei fenomeni del bullismo e del cyberbullismo*).

97 See more on the topic: Motta, 2020b.; Russo, 2022.

98 Act No. 71. of 2017 1. § (1-bis).

99 Act No. 70. of 2024 3. §.

Campania,¹⁰⁰ Lombardy¹⁰¹ and Piedmont.¹⁰² The provisions contained in this legislation – where offline bullying is also present, albeit only at regional level – mainly provide for the adoption of measures to prevent this phenomenon, such as campaigns, cultural or sporting events, training for teachers, and the creation of regional councils and action plans.¹⁰³

2.1. The instruments provided by the Act No. 71. of 2017 to fight cyberbullying

The Act No. 71. of 2017 provides two institutions for victims of cyberbullying, which can be used in cases of non-criminal behavior or to avoid prosecution.

A minor over the age of fourteen, the minor's parent or the person exercising parental authority may submit a request to the controller or the website or social media operator to erase, remove or block data of the minor that is disseminated on the Internet, identified by a URL, unless it constitutes prohibited processing¹⁰⁴ under the Code on the Protection of Personal Data.¹⁰⁵ Under the Code, the processing of personal data for commercial gain and to the detriment of others is punishable by imprisonment, unless a more serious offence is committed.¹⁰⁶ If, within twenty-four hours of receipt of the request, the requested controller or website operator does not declare that it will comply with the request or does not comply within forty-eight hours, or if the controller or media operator responsible cannot be identified, a complaint or a

100 Regional Act of Campania No. 11. of 2017 on provisions for preventing and combating the phenomenon of bullying and cyberbullying in the Campania Region (*Disposizioni per la prevenzione ed il contrasto dei fenomeni del bullismo e del cyberbullismo nella Regione Campania*).

101 Regional Act No. 1. of 2017 on discipline of regional interventions in preventing and combating bullying and cyberbullying (*Disciplina degli interventi regionali in materia di prevenzione e contrasto al fenomeno del bullismo e del cyberbullismo*).

102 Regional Act No. 2. of 2018 on provisions on preventing and combating the phenomenon of bullying and cyberbullying (*Disposizioni in materia di prevenzione e contrasto dei fenomeni del bullismo e del cyberbullismo*).

103 Giordano, 2019.; Rospi, 2017, pp. 474–475.

104 Trattamento illecito di dati.

105 Codice in materia di protezione dei dati personali (hereinafter: Code on the Protection of Personal Data).

106 Code on the Protection of Personal Data 167. §.

complaint may be submitted¹⁰⁷ to the Personal Data Protection Authority.¹⁰⁸ So this particular legal remedy¹⁰⁹ puts the responsibility for making harmful data or information inaccessible on the website operators.¹¹⁰ The interpretative provision of the Act No. 71. of 2017 defines website operators as all providers of Internet content on whose platform cyberbullying may occur.¹¹¹ Moreover, this generally and broadly defined concept is explicitly distinguished by the Act No. 71. of 2017 from the categories set out in the Legislative Decree 2003/70. The definition of a social media operator, which can be identified as a hosting service provider in the EU terminology, is not even specified.¹¹² For all these reasons, the definition of the website operator has been highly criticized.¹¹³ The issue of the fundamental rights conflict between the constitutional right to freedom of expression and the fight against cyberbullying has also been raised related to the removal of the offending data. It is up to the operator of the website to decide which content is illegal, for example harassment, defamation or pressure, and should be removed. In this ‘censorship’, the website operator can be neither too strict nor too permissive, as in the former case it would restrict freedom of expression and in the latter case it would not be in line with the legal policy intention to prevent cyberbullying.¹¹⁴ The time limit for the website operator to make this decision is extremely short.¹¹⁵ This short timeframe is, however, essential for effective action against cyberbullying, as the risk of harmful content spreading is increasing over time.¹¹⁶ However, under the law, in the absence of any substantive action by the data controller or website operator, it is possible to request the Personal Data Protection Authority to take action. The authority must deal with requests and complaints received within forty-eight hours of their receipt, after having established, in the course of a preliminary investigation, that the complaint or notification is well-founded and that the conditions for official action are met. Under the Code on the Protection of Personal Data, the decision of the Personal Data Protection Authority

¹⁰⁷ Act No. 71. of 2017 2. §.

¹⁰⁸ Garante per la protezione dei dati personali, also known as Garante della Privacy. It is an independent Italian administrative authority established by Act No. 675 of December 31, 1996, to ensure the protection of fundamental rights and freedoms and respect for dignity in the processing of personal data.

¹⁰⁹ Ricotta, 2017.

¹¹⁰ Gestore del sito internet.

¹¹¹ Act No. 71. of 2017 1. § (3).

¹¹² Bocchini, Montanari, 2018, pp. 356–365.; Colangelo, 2017, pp. 401–402.; Morelli, 2017.

¹¹³ Lásd például: Rospi, 2017, pp. 466–467.; Senor, 2017, p. 176.; Eremita, p. 8.

¹¹⁴ Benedetti, 2021, pp. 170–171.; Bocchini, Montanari, 2018, pp. 367–368.

¹¹⁵ Colangelo, 2017, p. 403.

¹¹⁶ Eremita, p. 10.

is subject to judicial remedy in the form of an appeal.¹¹⁷ So ultimately, a judicial forum can decide whether content posted online can be removed because it constitutes cyberbullying.

As long as no charges have been brought, Article 7 of the Act No. 71. of 2017 provides for the possibility to apply the warning procedure¹¹⁸ set out in the Decree-Law No. 11. of 23 February 2009 on urgent measures on public safety and combating sexual violence, as well as on persecutory acts (hereinafter: Decree-Law 2009/11.)¹¹⁹ in the event that a minor over the age of fourteen has committed an act of insult (Italian Criminal Code 594. §), defamation (Italian Criminal Code 595. §) or threat (Italian Criminal Code 612. §) online to the detriment of another minor. Or it is prohibited processing under the Code on the Protection of Personal Data.¹²⁰ Under the Decree-Law 2009/11., until a complaint is made under the Italian Criminal Code, the victim has the right to notify the public security authority of the facts and at the same time request that the perpetrator of the conduct be issued with a warning. Before issuing a warning, it is possible, if necessary, to ask the investigating authority for clarification or a statement of the facts. If, on this basis, the request is justified, the perpetrator of the offence complained of will be warned to comply with the law. The warning is usually verbal, but a record is made and a copy is given to the applicant and the person warned.¹²¹ The legislator's intention with regard to the applicability of the warning in the case of cyberbullying was clearly aimed at avoiding and preventing criminal proceedings.¹²² However, a number of questions have arisen in relation to the text of the legislation adopted. Thus, many were puzzled by the reference to the defamation stipulated by the Article 594 of Italian Criminal Code. This criminal offence was deleted from the Italian Criminal Code in 2016. This means that it had been out of force for more than a year at the time of the adoption of the Act No. 71. of 2017. (The provision can still be found in the current text of the Act No. 71. of 2017.) Moreover, some of these criminal offences – qualified threats and unlawful processing of data – are prosecutable *ex officio*, i.e. the

117 Code on the Protection of Personal Data 143–144. §; See more on the topic: Bocchini, Montanari, 2018, pp. 372–376.

118 Ammonimento.

119 Decreto-legge 23 febbraio 2009, n. 11: Misure urgenti in materia di sicurezza pubblica e di contrasto alla violenza sessuale, nonché in tema di atti persecutori (hereinafter: Decree-Law 2009/11.).

120 Act No. 71. of 2017 7. §. See more on the topic: Bocchini, Montanari, 2018, pp. 379–381; Colangelo, 2017, pp. 410–412; Eremita, 2018, pp. 10–12.

121 Decree-Law 2009/11. 8. §.

122 Bocchini, Montanari, 2018, p. 379.

authorities are obliged to report them, and criminal proceedings are inevitable.¹²³ Some also felt that the Act No. 71. of 2017 should refer to other provisions of the Decree-Law 2009/11. that set out the consequences of the warning. And thus to have some form of sanction.¹²⁴

Public funds that can be used to combat cyberbullying are also worth mentioning. The Act No. 71. of 2017 allocated two hundred and three thousand euros a year for three years, until 2019, from the fund for combating child pornography on the Internet and protecting information technology infrastructure of national interest¹²⁵ to finance training in schools on safe internet use and cyberbullying prevention.¹²⁶ The state has provided financial support for these and similar purposes in the past. The 2022 budget¹²⁷ provided for the creation of a permanent fund¹²⁸ to combat cyberbullying. The permanent fund, set up by a decree of the Ministry of Education, provided two million euros to amateur sports clubs, educational institutions and associations for the protection of minors for the year 2022 to finance education for minors and their prevention and awareness-raising activities.¹²⁹ The provision of the law, as well as the permanent fund, has been the subject of opinions that underestimate the amount of financial resources made available. Given the scale of the problem, which affects a large part of society, it would require more financial intervention.¹³⁰

2.2. Criminal law relevance of cyberbullying

As already mentioned, the Italian Criminal Code does not establish cyberbullying (nor bullying) as a separate criminal offence, and although it seemed so for a long time during the legislative process, the adoption of the Act No. 71.

123 Senor, 2017, pp. 176–177.; Rospi, 2017, pp. 471–473.

124 Eremita, 2018, p. 12.

125 The fund for combating child pornography on the Internet and protecting information technology infrastructure of national interest (Fondo per il contrasto della pedopornografia su internet e per la protezione delle infrastrutture informatiche di interesse nazionale) was created by the Act No. 48. of 18 March 2008 on the ratification and execution of the Council of Europe Convention on Cybercrime, done at Budapest on 23 November 2001, and rules for adaptation of domestic law (Legge 18 marzo 2008, n. 48: Ratifica ed esecuzione della Convenzione del Consiglio d'Europa sulla criminalità informatica, fatta a Budapest il 23 novembre 2001, e norme di adeguamento dell'ordinamento interno).

126 Act No. 71. of 2017 6. §.

127 Legge 30 dicembre 2021, n. 234: Bilancio di previsione dello Stato per l'anno finanziario 2022 e bilancio pluriennale per il triennio 2022-2024 (hereinafter: Act. No. 234. of 2021).

128 Fondo permanente per il contrasto del fenomeno del cyberbullismo.

129 Act. No. 234. of 2021 1. § (671) – (674); Russo, 2022.

130 Russo, 2022.; Senor, 2017, p. 177.

of 2017 did not change this. The question may arise as to whether it is even a legitimate expectation to create a new criminal offence. Because – as the definition of the Act No. 71. of 2017 illustrates – there are so many different types and degrees of conduct of cyberbullying that to include them in a single criminal offence would only raise problems and questions. In contrast, there are a number of criminal offences in the Italian legal system that penalize acts and conduct that are typically cyberbullying or closely related to it.¹³¹ Harassment,¹³² extortion,¹³³ defamation¹³⁴ and identity theft or manipulation,¹³⁵ as defined by law, are all criminal offences punishable by fines or imprisonment. Illegal processing is punishable under the Code on the Protection of Personal Data as described above. The paragraph on the warning procedure also refers to the criminal offence of threatening,¹³⁶ which can also be punishable by imprisonment if committed, for example, in public or anonymously. In addition, there are a number of criminal offences which, although not explicitly referred to in the Act No. 71. of 2017, are nevertheless relevant in this context.

Thus, the criminal offence of persecution,¹³⁷ created by the Decree-Law 2009/11. and incorporated into the Italian Criminal Code,¹³⁸ should be highlighted. It provides that, unless a more serious criminal offence is committed, a person who, by repeated threats or harassment, causes persistent and severe anxiety or well-founded fear for the safety of himself or a close relative, or forces him to change his way of life, shall be punished with imprisonment. The criminal offence is more serious if it is committed by a person who has an emotional relationship with the victim. It is even more serious if the victim is a minor, a disabled person or a pregnant woman. It is also a qualified case if the act of persecution is committed by means of information technology or other electronic means. Therefore, it can be concluded that with the inclusion of this provision in the Italian Criminal Code, in addition to many other forms of persecution and harassment, a type of cyberbullying, or a way of cyberbullying (the so-called cyberstalking), was given criminal relevance as a qualified case, in a

131 See: Bocchini, Montanari, 2018, pp. 347–348.; Giordano, 2019.; Motta, 2020a.; Motta, 2020b.; Racca, 2018.; Villafrate, 2022.; Eremita, 2018, pp. 4–6.; Grandi, 2017, pp. 51–53.

132 Italian Criminal Code 660. § – *Molestia o disturbo alle persone*; See e. g.: Martorana, Sichi 2022.

133 Italian Criminal Code 629. § – *Estorsione*.

134 Italian Criminal Code 595. § – *Diffamazione*; See e. g.: Panattoni, 2020, pp. 310–314.

135 Italian Criminal Code 494. § – *Sostituzione di persona*.

136 Italian Criminal Code 612. § – *Minaccia*.

137 Italian Criminal Code 612-bis § – *Atti persecutori*.

138 See: Guerini, 2012, pp. 17–20.

common provision, long before the adoption of Act No. 71. of 2017.¹³⁹ Similarly, the criminal offence of distribution of images and videos with sexual content, introduced by the Act No. 69. of 19 July 2019 on the amendments to the Criminal Code, Code of Criminal Procedure, and other provisions on the protection of victims of domestic and gender-based violence,¹⁴⁰ should be noted. Under the legislation, which penalises the phenomenon known colloquially as revenge porn, anyone who sends, transmits, distributes or publishes images or videos with sexual content without the consent of the persons concerned after they have been taken or stolen can be fined or even imprisoned.¹⁴¹ But there are also offences of coercion,¹⁴² unlawful interference with privacy¹⁴³ and assault,¹⁴⁴ which are also punishable by imprisonment. In addition to the physical injury resulting from the assault, mental illness is also a result of which the criminal offence is committed. In the most serious cases, the offence of participating in suicide¹⁴⁵ may also arise if someone persuades someone else to commit suicide, reinforces someone else's suicidal intentions or in any way helps someone else to commit suicide. The punishment is more severe if the victim is a minor or under the age of fourteen, or if the victim is mentally handicapped or intoxicated or drunk.

3. Prevention of Cyberbullying

As mentioned above, in Italy the fight against cyberbullying focuses primarily on adequate information and education, which is clearly reflected in the legislation. For members of government and educational institutions, the Act No. 71 of 2017 sets out a number of duties and obligations aimed at preventing cyberbullying. These include the integrated action plan for the prevention of cyberbullying and the guidelines issued by the Ministry of Education at regular intervals.¹⁴⁶ The Act No. 71 of 2017 requires the Minister of Education and Merit to set up a

139 See more on this topic: Crisafi, 2021.; Foligno, 2016.; Cassani, 2018, pp. 1–6.; De Simone, 2013, pp. 7–17.; Guerini, 2012, pp. 25–39.

140 *Legge 19 luglio 2019, n. 69: Modifiche al codice penale, al codice di procedura penale e altre disposizioni in materia di tutela delle vittime di violenza domestica e di genere.*

141 See more on this topic: Buffagni, 2022.; Biarella, 2019.

142 Italian Criminal Code 611. § – *Violenza o minaccia per costringere a commettere un reato.*

143 Italian Criminal Code 615-bis § – *Interferenze illecite nella vita privata.*

144 Italian Criminal Code 582. § – *Lesione personale.*

145 Italian Criminal Code 580. § – *Istigazione o aiuto al suicidio.*

146 Rospi, 2017, pp. 462–464.

technical council to combat cyberbullying (and bullying).¹⁴⁷ In addition to the ministries,¹⁴⁸ the council is made up of representatives of authorities such as the Personal Data Protection Authority, the Child and Adolescent Authority,¹⁴⁹ the Communications Guarantee Authority¹⁵⁰ and associations for the protection of minors' rights.¹⁵¹ This council draws up an integrated action plan¹⁵² to combat cyberbullying (and bullying), in line with EU directives and the self-regulatory code adopted by the Ministry of Development, under the coordination of the Ministries of Education and Higher Education and Research. The integrated action plan includes and summarizes initiatives and campaigns to inform citizens about the phenomenon, threat and prevention of cyberbullying (and bullying) or about available remedies and other means.¹⁵³ Each year, the technical council is required to report on its activities to both chambers of Parliament.¹⁵⁴

In addition, every two years the Ministry of Education must adopt a policy on preventing and combating bullying and cyberbullying.¹⁵⁵ Such or similar guidelines have been issued by the Ministry in the past, as mentioned in the previous chapter, but the Act No. 71. of 2017 has reinforced this obligation. In line with Act No. 107 of 13 July 2015 on the reform of the national education and training system and proxy for the reorganization of existing legislative provisions,¹⁵⁶ the policy of the Ministry of Education should cover, among other things, the appropriate training of school staff and the role of students and alumni in the prevention of cyberbullying (and bullying) and the necessary educational measures.¹⁵⁷ The Act No. 71 of 2017 requires all schools to adopt an internal code for the prevention and counteraction of bullying and cyberbullying in accordance with the above mentioned ministerial policy and establish a permanent monitoring table with the representatives of students, teachers, families and experts.¹⁵⁸ The schools are also required to appoint a referent from

147 Before the entry into force of the Act No. 70. of 2024 the Prime Minister was required to set up this technical council.

148 Such as the Ministry of the Interior, the Ministry of Education and Merit, the Ministry of Labour and Social Policy, the Ministry of Justice, the Ministry of Business and Made in Italy and the Ministry of Health.

149 *Autorità garante per l'infanzia e l'adolescenza*.

150 *Autorità per le Garanzie nelle Comunicazioni*.

151 2017/71. tv. 3. § (1) bekezdés; Bocchini, Montanari, 2018, p. 382.

152 *Piano di azione integrato*.

153 Act No. 71. of 2017 3. § (2)–(5).

154 Act No. 71. of 2017 3. § (6).

155 Act No. 71. of 2017 4. § (1); Motta, 2020a.

156 *Legge 13 luglio 2015, n. 107: Riforma del sistema nazionale di istruzione e formazione e delega per il riordino delle disposizioni legislative vigenti*.

157 Act No. 71. of 2017 4. § (2).

158 Act No. 71. of 2017 4. § (2-bis).

among teachers to coordinate initiatives to prevent and combat cyberbullying.¹⁵⁹ In addition, all educational institutions are obliged to educate and train pupils to be aware of their rights and obligations when using the Internet and information technologies.¹⁶⁰ It is also noteworthy that the Act No. 70 of 2024 established the institution of psychological support service for students.¹⁶¹ Under the newly adopted section of the Act No. 71. of 2017 the regions may adopt initiatives to ensure the provision of psychological support services for students at all levels of education.¹⁶²

Furthermore, the Act No. 70 of 2024 designated 20 January as the Day of Respect¹⁶³ which is also of great and symbolic importance in the prevention of cyberbullying. According to the provision of the act this day is a designated period for examining the tenets of mutual respect, fostering consciousness of the tenets of psychological and physical nonviolence, and combating all forms of discrimination.¹⁶⁴

The Ministry of Education's 2021 Guidelines for preventing and combating cyberbullying sets out the requirements for school sanctions for cyberbullying. The guideline sets out the measures that educational institutions can take to combat bullying and cyberbullying. These are divided into two groups. The assessment and monitoring of pupils at risk, the identification of harmful behaviour and appropriate training and information for both teachers and pupils are included as priority measures. Detecting bullying and cyberbullying through questionnaires, setting up a school reporting system, setting up a prevention task force and providing psychological support are among the measures advised. The guideline also outlines three levels of prevention, providing examples of actions and measures that could be taken in relation to bullying and cyberbullying. The primary or universal prevention would be to raise the awareness of the whole population, which could also be reflected in the curricula of schools. This could be achieved through compulsory reading, various discussion evenings or even events to strengthen classroom community. Secondary prevention activities should target vulnerable groups or people who have already been victims of bullying. To this end, schools should have an intervention plan in order to address the threat as early as possible, in cooperation with local professional services, teachers, parents and even students, at the earliest possible stage of bullying.

¹⁵⁹ Act No. 71. of 2017 4. § (3).

¹⁶⁰ Act No. 71. of 2017 4. § (5).

¹⁶¹ Servizio di sostegno psicologico agli student.

¹⁶² Act No. 71. of 2017 4-bis §.

¹⁶³ Giornata del rispetto.

¹⁶⁴ Act No. 70. of 2024 4. §.

Tertiary prevention measures should target groups where bullying or cyberbullying is present. A reporting system should be in place to detect acute or urgent situations. In schools, operational teams of appropriately trained persons should thoroughly investigate situations, decide on the most appropriate action to take and monitor the situation and intervention. The guideline foresees the creation of anti-bullying and emergency teams for schools. The former should be composed of the head teacher, the teacher designated as a referent, and other professionals such as a school psychologist, a specialist teacher or a health worker, while the latter would facilitate cooperation with other educational institutions or even law enforcement agencies. Both teams have the task of assisting the school principal in the prevention of bullying and cyberbullying and the implementation of intervention measures. At the end of each school year, the anti-bullying team is required to report relevant cases and their number to the regionally designated referent. The guideline is accompanied by two annexes. The first annex sets out in detail the intervention protocol to be followed by schools in dealing with acute situations, covering the behaviour to be adopted in relation to the victim, the perpetrator or group of perpetrators. The second annex contains recommendations for school staff and sets out their responsibilities.

In this context, it should be mentioned that on its official website, the Ministry of Education and Merit provides a detailed description of bullying and cyberbullying, juxtaposing the two definitions,¹⁶⁵ and that several NGOs are also carrying out similar outreach activities. Among the latter, the website *bullismo*.it provides a comprehensive and highly illustrative description of the phenomenon of bullying and cyberbullying, with specific reference to the legal and other tools available to victims.

4. Prevention and Responsibilities of Service Providers and Schools

With regard to the liability of service providers, it is worth recalling and briefly reiterating what has been written above. The Act No. 71 of 2017 gives victims of cyberbullying – or their parents – the right to have offensive content posted online removed or otherwise made inaccessible. The law obliges the website or social media operator to remove or make inaccessible the data concerned

¹⁶⁵ The Ministry of Education's briefing on bullying and cyberbullying is available: <https://www.miur.gov.it/bullismo-e-cyberbullismo>.

on the basis of a request received, if it considers the request to be justified. So, the operator of the website, which is defined by law as any provider of internet content on which cyberbullying may occur, has the right to determine whether the information or opinion posted constitutes cyberbullying. Although it is possible to request the intervention of the Personal Data Protection Authority in the event of inaction or refusal to remove the data, and the decision at the end of the procedure can be appealed in court, the primary role of the website operator is unquestionable. This solution has been highly criticized, considering that such decisions should not be left to these service providers. In addition, the definition under the Act No. 71 of 2017 is not in line with the concepts of EU legislation.

It is also important to address the issue of the responsibility of schools. According to the Act No. 71 of 2017, the school principal is obliged to notify the parents, guardians or persons exercising parental authority of the minors concerned and to take the necessary educational measures if he or she becomes aware of an act of cyberbullying that does not constitute a criminal offence.¹⁶⁶ Educational establishments are required to include in their rules¹⁶⁷ disciplinary sanctions for conduct that constitutes cyberbullying, proportionate to the seriousness of the offence.¹⁶⁸ According to the Ministry of Education's 2021 Guidelines for preventing and combating cyberbullying, these sanctions are primarily aimed at compensating for the damage caused and remedying the situation. The basic function of the sanctions is to make the offender realise the seriousness of his behaviour. The autonomy of the school is respected in the detailed development of the rules for combating bullying and cyberbullying, including the definition of sanctions. The head teacher is authorised to draw up this policy in conjunction with the teacher designated as the bullying and cyberbullying referent. These disciplinary measures must be included in the school rules approved by the school board, as well as in the responsibility agreement¹⁶⁹ signed by parents and children at enrolment, which sets out the rights and obligations of the school, parents and students. This information should also be published on the school website. Faculty members and school staff are required to report any bullying or cyberbullying incidents of which they become aware, directly or indirectly, to the principal, the referent or the bullying team and to initiate intervention. The teacher designated as the bullying referent works

¹⁶⁶ Act No. 71. of 2017 5. § (1); Berlingò, 2018, p. 11.; Rospi, 2017, p. 471.

¹⁶⁷ 4. § of Presidential Decree No. 249. of June 24 June 1998 on regulations on the status of secondary school students (*Decreto del Presidente della Repubblica 24 giugno 1998, n. 249: Regolamento recante lo statuto delle studentesse e degli studenti della scuola secondaria*, hereinafter: Presidential Decree 1998/249.).

¹⁶⁸ Act No. 71. of 2017 5. § (2).

¹⁶⁹ *Patto educativo di corresponsabilità*, see: Presidential Decree 1998/249. 5-bis §.

with the teaching staff, organises them training courses, assists the principal in developing a prevention protocol, monitors the handling of cases and liaises with the regional and district level authorities.

Many have assessed¹⁷⁰ that the provisions of the Act No. 71 of 2017 on the liability of schools are in line with the rules of the Italian Civil Code.¹⁷¹ Under the latter, teachers are liable for any damage caused by their students while under their supervision, unless they can prove that they could not have prevented the act.¹⁷² Although these rules are more relevant to the ‘traditional’ version of bullying, they fit well with the principal’s duty to notify and take action, and the duty of teachers and other staff to report, as set out in ministerial guideline.

Summary

It can be stated that the issues of hate speech and cyberbullying, as well as the measures to combat them, are both very current in Italy. Both phenomena are, and have been in recent years, the subject of constant legislative amendments and updating in line with the requirements of the times. The legal concept of bullying has recently been codified into law. In particular, the coronavirus pandemic has recently led to a significant increase in the number of such cases. In the context of the pandemic and its management, it is the polarized public discourse that has led to an increase in what can be considered hate speech. The rapid spread of the phenomenon of cyberbullying has been facilitated by the fact that, thanks to various quarantine measures, a significant part of human interaction has moved online.¹⁷³ The adoption of a law amending or supplementing the current legislation is therefore expected in relation to both phenomena. For example the criminalization of hate speech based on gender identity or sexual orientation. The issue of the responsibility of social media and online service providers in relation to hate speech is even more of an issue to be addressed. It is interesting to note that while in the case of cyberbullying the role of website operators is clearly defined by the Act No. 71 of 2017, in the case of hate speech only the relevant EU directive can be invoked, with several solutions being found

170 Benedetti, 2021, 171–172. pp.; Bocchini, Montanari, 2018, p. 348.

171 *Codice civile* (hereinafter: Italian Civil Code).

172 Italian Civil Code 2048. §.

173 See: Santerini, 2021, 155. p.; D’Amico, Fiano, 2021. pp. 134–135; Racca 2018; Cardinale, 2020.

in the case law of the EU courts. At the same time, both phenomena repeatedly raise the issue of the restriction of the right to freedom of expression.

It can therefore be concluded that, although the legal regulation of hate speech and, in particular, cyberbullying in Italy is noteworthy and commendable, there is still work to be done by the legislator.

Bibliography

- Abbondante, F. (2017) 'Il ruolo dei social network nella lotta all'hate speech: un'analisi comparata fra l'esperienza statunitense e quella europea' *Informatica e diritto*, 26(1-2), pp. 41-68
- Basile, F. (2019) 'Ti odio, "in nome di Dio". L'incriminazione dell'odio e della discriminazione (in particolare, per motivi religiosi) nella legislazione italiana', *Diritto Penale e Uomo*, 2019/12, pp. 1-13
- Benedetti, A. M. (2021) 'Minori "buoni" e minori "cattivi" nella nuova disciplina sul cyberbullismo', in Bianca, M. (ed.) *The best interest of the child*. Rome: Sapienza Università Editrice. pp. 165-177
- Berlingò, V. (2018) 'Le politiche pubbliche di contrasto e prevenzione del (bullismo e del) cyberbullismo nell'ordinamento italiano: art. 31, comma 2, Cost. e "servizio scolastico di periferia"', *Forum di Quaderni Costituzionali*, 2018/3, pp. 1-17.
- Biarella, L. (2019) *Codice Rosso: definizione, procedura, nuovi reati e aggravanti* [Online]. Available at: <https://www.altalex.com/documents/leggi/2019/07/26/codice-rosso#tre>
- Biffa, M. (2024) *La nuova legge per la prevenzione ed il contrasto del bullismo e del cyberbullismo* [Online]. Available at: <https://www.dippol.it/la-nuova-legge-per-la-prevenzione-ed-il-contrasto-del-bullismo-e-del-cyberbullismo/>
- Bocchini, R., Montanari, M. (2018) 'Le nuove disposizioni a tutela dei minori per la prevenzione ed il contrasto del fenomeno del cyberbullismo', *Nuove leggi civili commentate*, 2018/2, pp. 340-384
- Buffagni, E. (2022) *L'intimità digitale e le sue violazioni: il revenge porn* [Online]. Available at: <https://www.altalex.com/documents/news/2022/02/10/intimita-digitale-e-le-sue-violazioni-revenge-porn>
- Cardinale, R. L. (2020) *Il cyberbullismo ai tempi del coronavirus* [Online]. Available at: <https://www.altalex.com/documents/news/2020/12/30/cyberbullismo-ai-tempi-del-coronavirus>
- Cassani, C. (2018) 'Atti persecutori e recenti modifiche normative: spunti di riflessione', *Archivio penale*, 2018/1, pp. 1-13
- Castellani, L. (2021) *E-hate speech e funzione dell'Internet Service Provider*, Verona: Università di Verona: Osservatorio Cybercrime. pp. 1-26
- Colangelo, R. M. (2017) 'La legge sul cyberbullismo. Considerazioni informatico-giuridiche e comparatistiche', *Informatica e diritto*, 26(1-2), pp. 397-418
- Crisafi, M. (2021) *Il reato di Stalking o atti persecutori* [Online]. Available at: <https://www.studiocataldi.it/articoli/12949-il-reato-di-stalking.asp>
- D'Amico, M., Fiano, N. (2021) 'La Costituzione non odia: sui limiti costituzionali ai discorsi di odio', in D'Amico, M., Brambilla, M., Crestani, V., Fiano N.

- (eds.) *Il linguaggio dell'odio. Fra memoria e attualità*. Milan: Franco Angeli. pp. 125–141
- De Simone, G. (2013) 'Il delitto di atti persecutori (la struttura oggettiva della fattispecie)', *Archivio penale*, 2013/3, pp. 1–52
- Di Tano, F. (2017) 'Prospettive de iure condendo sulla responsabilizzazione dei content provider' *Informatica e diritto*, 26 (1–2) pp. 113–126
- Donati, F. (2019) 'La tutela dei minori nella direttiva 2018/1808', 2019/1, *MediaLaws – Rivista di diritto dei media*, pp. 60–72
- Egresi, K. (2013) *Az olasz alkotmány*. Budapest: Gondolat Kiadó.
- Eremita, A. R. (2018) 'Tutela del minore e cyberbullismo: Note a prima lettura della L. 71/2017', *La Nuova Procedura Civile*, 2018/3, pp. 1–14
- Falletta, P. (2020) 'Controlli e responsabilità dei social network sui discorsi d'odio online', *MediaLaws – Rivista di diritto dei media*, 2020/1, pp. 146–158
- Fierimonte, E. (2022) *Cyberbullismo e social network* [Online]. Available at: <https://www.studiocataldi.it/articoli/44203-cyberbullismo-e-social-network.asp#par5>
- Focaroli, R. (2020) *Legge contro il cyberbullismo: una speranza rimasta tale* [Online]. Available at: <https://www.studiocataldi.it/articoli/40554-legge-contro-il-cyberbullismo-una-speranza-rimasta-tale.asp>
- Foligno, E. (2016) *Le prove dello stalking* [Online]. Available at: <https://www.studiocataldi.it/articoli/19706-stalking-aspetti-psicologici-e-prove.asp>
- Giordano, A. (2019) *Cyberbullismo: profili normativi e giurisprudenziali* [Online]. Available at: <https://www.studiocataldi.it/articoli/33438-cyberbullismo-profil-normativi-e-giurisprudenziali.asp#par2>
- Giordano, A. (2024) *Bullismo e cyberbullismo: cosa prevede la legge 70/2024* [Online]. Available at: <https://www.studiocataldi.it/articoli/46838-bullismo-e-cyberbullismo-cosa-prevede-la-legge-702024.asp>
- Grandi, C. (2017) 'Le conseguenze penalistiche delle condotte di cyberbullismo. Un'analisi de jure condito', *Annali online della Didattica e della Formazione Docente*, 9(13), 40–58. pp.
- Guerini, T. (2012) 'Il delitto di atti persecutori. Tra carenza di determinatezza e marketing penale', *Studi e materiali di diritto penale*, 5(2), pp. 17–46
- Leoni, A. (2016) *L'evoluzione del contrasto all'hate speech tra online ed offline*. Rome: LUISS Guido Carli
- Liberati, B. (2015) 'L'educazione e la prospettiva del "rispetto dei generi" quale strumento per contrastare la violenza e il bullismo', *Osservatorio Costituzionale*, 2015/3, pp. 1–30
- Manna, M. (2020) *Facebook vs. CasaPound: the deactivation of CasaPound's page and account is unlawful* [Online]. Available at: <https://www.martinimanna.>

- com/blog/facebook-vs-casapound-the-deactivation-of-casapounds-page-and-account-is-unlawful
- Marsocci, P. (2021) 'Discorsi d'odio online e tutela costituzionale dei minori' in Bianca, M. (ed.) *The best interest of the child*. Rome: Sapienza Università Editrice, pp. 215–230
- Martorana, M., Sichi, Z. (2021) Cyberbullismo: cosa succede se mio figlio ne è vittima? Quali tutele? [Online]. Available at: <https://www.altalex.com/documents/news/2021/03/30/cyberbullismo-cosa-succede-se-mio-figlio-ne-e-vittima-quali-tutele>
- Martorana, M., Sichi, Z. (2022) Il Metaverso e il reato di molestie sessuali nella realtà virtuale [Online]. Available at: <https://www.altalex.com/documents/news/2022/02/23/il-metaverso-e-il-reato-di-molestie-sessuali-nella-realta-virtuale>
- Morelli, C. (2017) Cyberbullismo: provider fuori dal raggio d'azione della legge [Online]. Available at: <https://www.altalex.com/documents/news/2017/05/23/cyberbullismo>
- Motta, M. B. (2020a) Cyberbullismo: la guida completa [Online]. Available at: <https://www.altalex.com/guide/cyberbullismo>
- Motta, M. B. (2020b) Il bullismo [Online]. Available at: <https://www.altalex.com/guide/bullismo>
- Nardi, V. (2019) 'I discorsi d'odio nell'era digitale: Quale ruolo per l'internet service' *Diritto Penale Contemporaneo*, 2019/2, pp. 268–288
- Occhipinti, S. (2020) Legge sull'omotransfobia: il testo approvato alla Camera [Online]. Available at: <https://www.altalex.com/documents/leggi/2020/11/05/legge-sull-omotransfobia-il-testo-approvato-alla-camera>
- Panattoni, B (2020) 'I riflessi penali del perdurare nel tempo dei contenuti illeciti nel cyberspace', *Sistema Penale*, 2020/5, pp. 303–324
- Pulitanò, D. (2015) 'Di fronte al negazionismo e al discorso d'odio', *Diritto Penale Contemporaneo*, 2015/4, pp. 325–332
- Pulitanò, D. (2019) 'Legge penale, fascismo, pensiero ostile', *MediaLaws – Rivista di diritto dei media*, 2019/1, pp. 12–24
- Racca, A. (2018) Previsioni di contrasto ai fenomeni di cyber-bullismo nella L. 71/2017 [Online]. Available at: <https://www.dirittopenaleglobalizzazione.it/previsioni-contrasto-ai-fenomeni-cyber-bullismo-nella-l-712017-gazz-uff-n-127-del-03062017/>
- Ricotta, F. (2017) Cyberbullismo: riflessioni critiche sulla nuova legge [Online]. Available at: <https://www.altalex.com/documents/news/2016/10/12/cyber-bullismo>
- Rosato, A. S. S. (2016) 'Osservazioni critiche sul nuovo "reato" di negazionismo', *Diritto Penale Contemporaneo*, 2016/3. pp. 280–312

- Rospi, M. (2017) 'Social media, minori e cyberbullismo: lo status quo della legislazione nazionale ed eurounitaria', *Informatica e diritto*, 26(1-2), pp. 453-482
- Russo, P. (2022) Un Fondo per combattere il cyberbullismo nella Legge di Bilancio [Online]. Available at: <https://www.altalex.com/documents/2022/01/05/un-fondo-per-combattere-il-cyberbullismo-nella-legge-di-bilancio>
- Santerini, M. (2021) 'Pregiudizio antisemita e propaganda online', in D'Amico, M., Brambilla, M., Crestani, V., Fiano N. (eds.) *Il linguaggio dell'odio. Fra memoria e attualità*. Milan: Franco Angeli, pp. 143-158.
- Senor, M. A. (2017) 'Un primo commento alla legge sul cyberbullismo', *MediaLaws – Rivista di diritto dei media*, 2017/1, pp. 174 – 177
- Sorrentino, A., Baldry, A. C., Cacace, S. (2018) 'Cyberbullying in Italy', in Baldry, A. C., Blaya, C., (eds.) *International Perspectives on Cyberbullying. Prevalence, Risk Factors and Interventions*. London: Palgrave Macmillan, pp. 231-249
- Vallini, A. (2020) 'Criminalizzare l'hate speech', *Studi sulla questione criminale*, 15(1), pp. 33-64
- Venanzoni, A. (2019) Pluralismo politico e valore di spazio di dibattito pubblico della piattaforma social Facebook: la vicenda Casapound [Online]. Available at: <https://dirittodiinternet.it/pluralismo-politico-valore-spazio-dibattito-pubblico-della-piattaforma-social-facebook-la-vicenda-casapound-tribunale-civile-roma-sezione-specializzata-materia-dimpresa-ord/>
- Villafrate, A. (2022) Il cyberbullismo [Online]. Available at: <https://www.studiocataldi.it/articoli/32450-cyberbullismo.asp>
- Ziccardi, G. (2021) 'Le espressioni d'odio sulle piattaforme digitali: alcune considerazioni informatico-giuridiche', in D'Amico, M., Brambilla, M., Crestani, V., Fiano N. (eds.) *Il linguaggio dell'odio. Fra memoria e attualità*. Milan: Franco Angeli, pp. 159-182

