Enforcing rules on illegal content and disinformation online

IRIS

A publication
of the European Audiovisual Observatory

European Audiovisual Observatory

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

IRIS-6
Enforcing rules on illegal content and disinformation online
European Audiovisual Observatory, Strasbourg, 2025
ISSN 2079-1062

Director of publication – Pauline Durand-Vialle, Executive Director
Editorial supervision – Maja Cappello, Head of Department for Legal Information
European Audiovisual Observatory

Editorial team – Sophie Valais and Diego de la Vega
European Audiovisual Observatory

Authors (in alphabetical order)
Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt, Krzysztof Wojciechowski

Proofreading
Linda Byrne

Editorial Assistant – Alexandra Ross
Press and Public Relations – Alison Hindhaugh, alison.hindhaugh@coe.int
European Audiovisual Observatory

Publisher
European Audiovisual Observatory
76, allée de la Robertsau, 67000 Strasbourg, France
Tel.: +33 (0)3 90 21 60 00
iris.obs@coe.int
www.obs.coe.int

Cover layout – ALTRAN, France

Please quote this publication as
Cappello M. (ed.), *Enforcing rules on illegal content and disinformation online*, IRIS, European Audiovisual Observatory, Strasbourg, December 2025

To promote inclusive language, we follow the guidelines of the Council of Europe.

Enforcing rules on illegal content and disinformation online

Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt and Krzysztof Wojciechowski

European Audiovisual Observatory

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Foreword

"Absolute freedom mocks justice. Absolute justice denies freedom. To be fruitful, both concepts must find their limits in each other."[1] Albert Camus inserted this sentence in *The Rebel*, an essay published in 1951, just a few years after World War II and the Holocaust. This caused quite a stir among the so-called intellectuals of the time for his criticism of revolutionary movements and their excesses.

Around fifty years later, the Internet, yet another revolution that preached absolute freedom, inevitably brought with it its fair share of excesses that we are still paying for and fighting against today.

However, as Camus asserted, it is not possible to juxtapose absolute justice and absolute freedom in opposition; rather, both concepts must be balanced for them to be fruitful.

The concept of freedom of expression finds its limits in the interests of national security, territorial integrity or public safety, the prevention of disorder or crime, the protection of health or morals, the protection of the reputation or rights of others, in preventing the disclosure of information received in confidence, or in maintaining the authority and impartiality of the judiciary. Limitations in this regard must, however, be prescribed by law and be necessary in a democratic society.

As such, certain online content may be considered illegal and must be removed by the author or publisher, either voluntarily or after an administrative or a court decision. This, as complicated as it might sometimes be, is still a straightforward law enforcement operation. Then comes the tricky part: harmful content. As explained by the authors of the present publication, "harmful content encompasses material that may not be illegal but is nonetheless considered detrimental to individuals or society — for example, disinformation, health misinformation, or content that undermines democratic processes". Now, the question is how to fight against content that is not illegal, and therefore not limited by law? *Ay, there's the rub*.[2]

This report, elaborated in collaboration with the Institute of European Media Law (EMR), and experts in this complex field, offers a comprehensive approach to the enforcement of rules against illegal content and disinformation online. From the general framework of the European Union and the Council of Europe, and its platform regulation, the report provides an in-depth analysis of national examples from across Europe that illustrate the current situation regarding this matter.

I would like to warmly thank all authors contributing to this report for their engaged participation and excellent work (by order of chapter): Mark D. Cole, Sandra Schmitz-Berndt, Roxana Radu, William Gilles, Irène Bouhadana, Dariia Opryshko, Mehmet Bedii Kaya, Roderick Flynn, Clara Rauchegger, Giovanni de Gregorio, Krzysztof Wojciechowski and Mariette Jones.

---

[1] Camus, A., *L'Homme révolté* [The rebel], Gallimard, Folio essais,1951, p. 363.
[2] Shakespeare, W., *The Oxford Shakespeare: Hamlet,* Oxford University Press, 2008 reissue edition.

Now, without wanting to pre-empt the conclusions of this interesting report, let me conclude with a personal reflection. The task of regulating the online world may sometimes seem superhuman, and there is certainly so much more to be done, but let's not lose faith: quoting Albert Camus again, “we call tasks superhuman when they take people a long time to accomplish, that's all”.[3]

Enjoy the read!

Maja Cappello

IRIS Coordinator

Head of the Department for Legal Information

European Audiovisual Observatory

[3] Camus, A., *L'Été* [Summer], 1954, Quarto Gallimard, Œuvres, 2013.

Table of contents

List of abbreviations and acronyms

AEP	*Autoritatea Electorală Permanentă* (Permanent Electoral Authority, Romania)
AI	Artificial Intelligence
AGCOM	*Autorità per le Garanzie nelle Comunicazioni* (Communications Authority, Italy)
ANCOM	*Autoritatea Națională pentru Administrare și Reglementare în Comunicații* (National Authority for Management and Regulation in Communications, Romania)
APIs	Application Programming Interfaces
ARCOM	*Autorité de régulation de la communication audiovisuelle et numérique* (Regulatory authority for audiovisual and digital communication, France)
AS	Autonomous System
ASA	Advertising Standard Authority (UK)
AVMSD	Audiovisual Media Services Directive
BAI	Broadcasting Authority of Ireland
BGH	Bundesgerichtshof (Federal Supreme Court, Germany)
BKA	*Bundeskriminalamt (*Federal Police Office, Germany)
BNetzA	*Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railways, Germany)
BTK	*Bilgi Teknolojileri ve İletişim Kurumu* (Information and Communication Technologies Authority, Türkiye)
CAP	Committee of Advertising Practice (Ireland)
CDSM	Copyright in the Digital Single Market Directive
CFREU	Charter of Fundamental Rights of the European Union
CFSP	Common Foreign and Security Policy
CJEU	Court of Justice of the European Union
CM/Rec	Committee of Ministers/Recommendation
CNA	*Consiliul Național al Audiovizualului* (National Audiovisual Council, Romania)
CnaM	*Coimisiún na Meán* (Media Commission, Ireland)
CPS	Core Platform Services
DDG	*Digitale-Dienste-Gesetz* (Digital Services Law, Germany)
DMA	Digital Markets Act
DNS	Domain-Name-System

DPA	Data Protection Authority
DPI	Deep Packet Inspection
DSA	Digital Services Act
DSC	Digital Services Coordinator
EBDS	European Board for Digital Services
EBMS	European Board for Media Services
ECD	e-Commerce Directive
ECHR	European Convention on Human Rights
ECtHR	European Court of Human Rights
EDMO	European Digital Media Observatory
EDPB	European Data Protection Board
EEA	European Economic Area
EEAS	European External Action Service
EFCSN	European Fact-Checking Standards Network
EFTA	European Free Trade Association
EMFA	European Media Freedom Act
EMR	Institute of European Media Law
ERGA	European Regulators Group for Audiovisual Media Services
EU	European Union
EUDI	European digital identity
EUR	Euro
FIMI	Foreign Information Manipulation and Interference
FIMI-ISAC	Foreign Information Manipulation and Interference – Information Sharing and Analysis Centre
GDPR	General Data Protection Regulation
ICCPR	International Covenant on Civil and Political Rights
IPCR	Integrated Political Crisis Response
JMStV	*Jugendmedienschutz-Staatsvertrag* (Interstate Treaty on the protection of minors in the media, Germany)
JORF	*Journal officiel de la République française* (Official journal, France)
KAS	*Krajowa Administracja Skarbowa* (National revenue administration, Polen)
KDD	*Koordinator für digitale Dienste* (Digital services coordinator)

KDD-G	*Koordinator-für-Digitale-Dienste-Gesetz* (Digital services coordinator law, Austria)
KRRiT	*Krajowa Rada Radiofonii i Telewizji* (National broadcasting and television council, Poland)
KoPl-G	*Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen* (Federal Act on measures to protect users on communications platforms, Austria)
LCEN	*Loi pour la confiance dans l'économie numérique* (Law on confidence in the digital economy, France)
MStV	*Medienstaatsvertrag* (Interstate media treaty, Germany)
NaD	Network against Disinformation
NASK	*Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy* (Research and academic computer network – national research institute, Poland)
NCCC	National Cybersecurity Coordination Centre (Ukraine)
NCU	National Centre for Operational and Technical Management of Telecommunication Networks (Ukraine)
NetzDG	*Netzwerkdurchsetzungsgesetz* (Network enforcement law, Germany)
NSDC	National Security and Defense Council (Ukraine)
OJ	Official Journal of the EU
OSA	Online Safety Act (UK)
OSMR	Online Safety and Media Regulation (Ireland)
PACE	Parliamentary Assembly of the Council of Europe
PERCI	*Plateforme Européenne de Retraits de Contenus illégaux sur Internet* (European platform for the takedown of illegal content online)
PEReN	*Pôle d'Expertise de la Régulation Numérique* (Competence centre for the regulation of digital platforms, France)
RRS	Rapid Response System
StGB	*Strafgesetzbuch* (Deutschland/Österreich)
TerrOIBG	*Terroristische-Online-Inhalte-Bekämpfungsgesetz* (Law to combat terrorist content online, Germany)
TEU	Treaty on European Union
TCOR	Terrorist Content Online Regulation
TFEU	Treaty on the Functioning of the European Union
TTPAR	Transparency and Targeting of Political Advertising Regulation

UKE	*Urząd Komunikacji Elektronicznej* (Office of electronic communications, Poland)
UML	Media Law (Ukraine)
UN	United Nations
UŚUDE	*Ustawa o świadczeniu usług drogą elektroniczną* (Act on provision of services by electronic means, Poland)
VIGINUM	*Service de vigilance et de protection contre les ingérences numériques étrangères* (Service for the surveillance of and protection against foreign digital interference, France)
VLOP	Very Large Online Platform
VLOSE	Very Large Online Search Engine
VLOPSEs	(VLOPs and VLOSEs)
VOD	Video on demand
VPN	Virtual Private Network
VSP	Video-Sharing Platform
VwVG	*Verwaltungsvollstreckungsgesetz* (Adminstrative enforcement Act, Germany)
ZMI	Central Reporting Office for Criminal Content on the Internet (Germany)
ZPO	*Zivilprozessordnung* (Code of civil procedure, Austria)

Executive Summary

This IRIS report offers a comprehensive analysis of the current enforcement of European rules on illegal content and disinformation online. Twelve distinguished authors,[4] experts in their respective fields, have contributed with chapters that explore both at a European and national level how regulatory frameworks can enforce the existing rules.

The report offers not only the angle of the European Union and Council of Europe, but also a variety of national examples useful for understanding what is being done today to address this crucial question across Europe.

Chapter 1, authored by Mark D. Cole and Sandra Schmitz-Berndt, focuses on how digital platforms are powerful tools for expression but also represent unique risks due to their market power, their reach, and the lack of editorial control. The chapter also delves into the differences between illegal content and disinformation online, exploring the legal aspects of each concept, their dissemination, and the nuances that can be found in different European countries.

Chapter 2 explores the legal framework on content regulation and the enforcement measures that are foreseen in the European framework. The first section, authored by Sandra Schmitz-Berndt, analyses the enforcement measures and the fundamental rights framework of the Council of Europe, taking into account not only the various recommendations issued by the institution and the Resolutions from the Parliamentary Assembly of the Council of Europe (PACE), but also the case law from the European Court of Human Rights (ECtHR).

From the idea that the Internet plays an important role for the exercise of the right to freedom of expression, the author analyses the liability of Internet portals as well as the duties and responsibilities of Internet intermediaries as well as non-professional entities and creators of hyperlinks regarding unlawful third-party content. The author also looks at the different enforcement measures in view of the case law of the Court, like blocking access to websites or social media accounts.

The second section sets out the framework on content regulation and the enforcement measures taken on the European Union (EU) level, especially in primary law and under the Common Foreign and Security Policy (CFSP) and in connection with foreign information manipulation and interference (FIMI). The chapter presents other tools

[4] In alphabetical order: Irène Bouhadana, Mark D. Cole, Roderick Flynn, William Gilles, Giovanni de Gregorio, Mariette Jones, Mehmet Bedii Kaya, Dariia Opryshko, Roxana Radu, Clara Rauchegger, Sandra Schmitz-Berndt and Krzysztof Wojciechowski.

designed by the EU to address enforcement of measures targeting illegal content and disinformation.

In **Chapter 3**, Mark D. Cole explores the enforcement measures against disinformation at the EU level and focuses on state-driven disinformation as an example of how the scale and quality of disinformation campaigns have intensified in the EU. The author also analyses European initiatives like the EU Code of Practice on Disinformation and how it relates to the Digital Services Act (DSA) and takes a look at tools like fact-checking and engaging trusted flaggers in the digital environment.

This chapter includes a section by Roxana Radu on Romania, exploring the national framework concerning platforms, specific rules regarding disinformation and the particular case of the annulment of Romania's 2024 presidential election, where disinformation played a key role in compromising the electoral process, building on deeper structural vulnerabilities, including political instability, economic uncertainty, and societal polarisation. William Gilles and Irène Bouhadana examine the example of France, from the national legal framework concerning platforms, framed by constitutional case law, to specific rules regarding disinformation and their application in the case of recent elections.

Also in this chapter, Dariia Opryshko offers an overview of the situation in Ukraine, examining the national legal framework concerning platforms and the new Ukrainian Media Law. It explores the specific rules introduced by this law regarding disinformation and their application in the case of foreign interference by disinformation in the context of the war. The chapter also explores how the lack of effective mechanisms to counter influence from foreign online platforms in order to protect its national interests has led to widespread blocking of websites and online platforms.

In **Chapter 4**, Mark D. Cole focuses on the accessibility of terrorist content and measures taken to counter this from the perspective of the Terrorist Content Online Regulation (TCOR), which includes "removal orders" and empowers competent authorities to issue such orders requiring hosting providers to remove terrorist content or disable access to terrorist content in all EU member states.

Also in this chapter, Sandra Schmitz-Berndt presents the current German framework concerning platforms while paying attention to the now derogated *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act – NetzDG) and its principles that inspired the DSA. The NetzDG already provided a list of criminal offences that constituted "unlawful content" and imposed upon social network providers an obligation to maintain an effective and transparent procedure for handling complaints about such unlawful content. The chapter also examines the specific German rules regarding terrorist content.

Mehmet Bedii Kaya offers insight into the situation in Türkiye, providing an overview of the national legal framework concerning platforms from the point of view of the Turkish membership of the Council of Europe and the candidacy to the European Union. As explained by the author, Türkiye has developed a comprehensive regulatory infrastructure aimed at preserving public order across both physical and digital domains and some specific rules regarding terrorist content.

In **Chapter 5**, Mark D. Cole focuses on countering defamatory, hateful and violence-inciting speech, from the perspective of the enforcement at the EU level. Alongside this

analysis, Roderick Flynn delves into the Irish framework concerning online platforms and the role of the new media regulator *Coimisiún na Meán* (CnaM). The author analyses the transposition process of the DSA in this regard and the specific rules regarding defamatory, hateful and violence-inciting speech along with the Irish Online Safety Code.

Clara Rauchegger presents the situation in Austria, in particular the Austrian Communication Platforms Act and the ensuing case law from the Court of Justice of the European Union (CJEU), and how this has influenced the interpretation of the DSA. The author also examines the application of the Austrian framework in cases of cyber harassment and image-based sexual abuse.

Giovanni de Gregorio offers the example of Italy, explaining the national mechanisms for enforcing the provisions of the DSA, the specific rules regarding defamatory, hateful and violence-inciting speech and the role played by the *Codice Penale* (Criminal Code). The author also presents the judicial enforcement mechanisms in place and includes an analysis of the remaining challenges to this.

In **Chapter 6**, Mark D. Cole takes a look at other areas of harmful content, specifically content that is not necessarily unlawful but may, nonetheless, be subject to access restrictions for specific groups and, in particular, minors as the content may be harmful to them especially through audiovisual means.

In this chapter, Krzysztof Wojciechowski explains in detail the case of Poland and the very recent reforms concerning harmful content, analysing the difficulties experienced from a legislative and judicial point of view to address this complex matter.

Mariette Jones presents the situation in the UK, particularly with regard to the Online Safety Act, which became law in September 2023, which compels private companies to actively monitor, evaluate, and remove harmful content created by third parties and take measures to protect children from such content, such as enhanced age verification. Also, this section takes a look at online gambling.

Finally, in **Chapter 7**, Mark D. Cole and Sandra Schmitz-Berndt provide a comparative analysis of the case-studies presented by the national reports, highlighting the variations in how law enforcement is applied to Internet intermediaries across Europe. Although EU legislation has driven substantial harmonisation directly binding for its member states, the differences in how law enforcement is applied to Internet intermediaries across Europe persist.

1. Introduction and overview

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg, and Dr Sandra Schmitz-Berndt, Research Associate, Institute of European Media Law (EMR)

In the digital age, the Internet serves as an "unprecedented platform for the exercise of freedom of expression"[5] and has become an "essential tool for participation in activities and discussions concerning political issues and issues of general interest".[6] It thereby plays an important role in enhancing the public's access to news and, more generally, facilitates the dissemination of information in real time and on a global scale.[7] Notably, the evolution of the Internet has been marked by a profound shift from a static information-retrieval tool to a dynamic participatory space that empowers individuals to create, share, and engage with content on a new scale and with potential global reach.

Early stages of the Internet were primarily characterised by one-way communication (Web 1.0), where users consumed information provided by a limited number of sources. This also meant that the source of illegal content, i.e. the original perpetrator or at least someone responsible for a certain website, could be identified and theoretically held accountable. Obviously, already at this stage the "borderless" nature of the Internet presented challenges that remain today: identification of the person or entity against whom enforcement is sought, jurisdictional questions, applicability of national law and ultimately, enforcement in cross-border cases.[8] Over time, the rise of Web 2.0 technologies in a bidirectional communication and social media platforms in the early 2000s transformed the Internet into an interactive environment, enabling ordinary users to become content creators, commentators, and community builders. This participatory turn has democratised

[5] *Delfi As v. Estonia [GC]*, Application No. 64569/09 (ECtHR, 16 June 2015), paragraph 110; *Times Newspapers Ltd (Nos. 1 & 2) v. the United Kingdom*, Application Nos. 3002/03 and 23676/03 (ECtHR, 10 March 2009), paragraph 27; and *Ahmet Yildirim v. Turkey*, Application No. 3111/10 (ECtHR, 18 December 2012), paragraph 48.

[6] *Sanchez v. France*, No. 45581/15 (ECtHR [GC], 15 May 2023), paragraph 158 with reference to *Vladimir Kharitonov v. Russia*, Application No. 10795/14 (ECtHR, 23 June 2020), paragraph 33 and *Melike v. Turkey*, Application No. 35786/19 (ECtHR, 15 June 2021), paragraph 44.

[7] *Sanchez v. France*, op. cit., paragraph 159; *Delfi AS v. Estonia [GC]*, op. cit., paragraph 133.

[8] See Reed C., *Making Laws for Cyberspace*, Oxford University Press, Oxford, 2012, pp. 49 et seq; Cole M.D., Etteldorf C. and Ullrich C., *Cross-Border Dissemination of Online Content*, Bd. 81 Schriftenreihe Medienforschung, Nomos, Baden-Baden, 2021, pp. 221 et seq; Cole, M.D. and Etteldorf, C., *Future Regulation of Cross-Border Audiovisual Content Dissemination*, Bd. 83 Schriftenreihe Medienforschung, Nomos, Baden-Baden, 2023, pp. 85 et seq; Ukrow J., "Framework for Law Enforcement against Online and Foreign Content Providers" in Cappello M. (ed.), *Media Law Enforcement without Frontiers*, *IRIS Special*, European Audiovisual Observatory, Strasbourg, 2018, pp. 9 et seq.

public discourse,[9] allowing diverse voices to contribute to political, cultural, and social conversations that were once dominated by traditional media and institutional actors.[10] It has also fostered new forms of civic engagement, activism, and information exchange, reinforcing the Internet's role as a cornerstone of modern democratic life.

While the ethos of Web 2.0 was one of openness, participation and decentralised innovation, this participatory infrastructure became dominated by a handful of large online platforms. The emergence of platforms as central actors in the digital ecosystem has fundamentally transformed how information is produced, distributed, and consumed, positioning them as powerful gatekeepers in the online public sphere. Although they continue to enable participation, as data-driven business models they increasingly engage in algorithmic curation of content and shape what content is seen, shared or even removed. This means that their prior status of mere passive intermediaries hosting third-party content becomes increasingly blurred and with some features they are taking a more active role meaning that liability models which had emerged under Web 2.0 are being put to the test.[11] The increased interference with content raises new issues about transparency, accountability, and the protection of fundamental rights in the digital sphere. In view of the gatekeeping power of platforms, new enforcement models aimed at the removal and disabling of access to illegal and harmful content are emerging, and these have been criticised by some, for instance the owner of X, Elon Musk, as "censoring speech".[12]

Significantly, the very features that make digital platforms powerful tools for expression — ease, speed, reach, and permanence — also distinguish them from traditional forms of media in ways that create unique risks due to their market power, their reach, and the lack of editorial control. Harmful or illegal content can be "disseminated as never before, worldwide, in a matter of seconds", and may remain accessible online indefinitely.[13] Accordingly, responsible and diligent behaviour by platform providers as well as any provider of intermediary services is essential for a safe, predictable and trustworthy online environment and for allowing users to exercise their fundamental rights as guaranteed in fundamental rights frameworks, in particular freedom of expression and freedom of information, the freedom to conduct a business, the right to non-discrimination and the attainment of a high level of consumer protection.[14] This being said, rules against illegal and harmful content must not focus solely on platforms; they need to consider the wide range of actors performing diverse roles in the creation, dissemination, and moderation of

[9] See Rowland D., Kohl U. and Charlesworth A., *Information Technology Law*, Routledge Abingdon, 5th ed. 2017, pp. 9 et seq.
[10] See *Sanchez v. France [GC]*, op. cit., paragraph 159; *Delfi As v. Estonia [GC]*, op. cit., paragraph 133.
[11] Cole M.D., Etteldorf C. and Ullrich C., *Cross-Border Dissemination of Online Content*, op. cit., pp. 41 et seq.
[12] See Elon Musk's statement on X of 12 July 2024. In the same sense, the current U.S. government is considering sanctions on EU or member state officials responsible for implementing the DSA, see Pamuk H., "Exclusive: Trump Administration Weighs Sanctions on Officials Implementing EU Tech Law, Sources Say", Reuters, 26 August 2025. Similarly, the U.S. Vice President J.D. Vance accused EU politicians of censoring free speech during his speech at the Munich Security Conference, see Bose, N. and Chiacu, D., "In Munich, Vance Accuses European Politicians of Censoring Free Speech", Reuters, 14 February 2025.
[13] *Sanchez v. France [GC]*, op. cit. (paragraph 160 with reference to *Savva Terentyev v. Russia*, Application No. 10692/09 (ECtHR, 28 August 2018), paragraph 79, and *Savcı Çengel v. Turkey*, Application No. 30697/19 (ECtHR, 18 May 2021), paragraph 35.
[14] Cf. Recital 3 DSA.

content. Legal and normative frameworks have been lagging behind the complex challenge of protecting fundamental rights and societal interests in cyberspace. On a global level, limited solutions for tackling illegal content online exist.[15] Even within the relatively coherent European legal space, harmonisation of media content regulation remains partial but, as regards the EU, has recently moved a significant step forward with several digital legal acts that address the dissemination of illegal and harmful content directly or indirectly.

This report focuses on the enforcement of rules against illegal content and disinformation online. While both categories of content are highly relevant, *inter alia*, to societal resilience and democratic integrity, they differ in important legal and conceptual ways — particularly with respect to what types of online speech may legitimately be restricted. In that regard, it becomes necessary to clarify the terminology.

In this publication, illegal content refers to material that violates existing statutory legal provisions. Its illegality is clearly defined by statute or case law. Accordingly, what is illegal is predominantly subject to national law. In turn, this already highlights one of the challenges, namely the limitations on enforcement where there is a lack of definitional harmonisation across national laws when it comes to what is considered illegal and how this issue can be resolved even at a supranational level such as the EU level. However, due to the common understanding of the notion "illegal", this notion is used in the publication rather than the broader and less precisely defined term "unlawful content". Some laws, in particular at national level, may refer to "unlawful content" such as, for instance, the (partly abrogated) German NetzDG.[16] Unlawful content includes illegal content but may also cover actions or material that are in breach of administrative norms, contractual obligations or regulatory standards. For legal precision, the standard legal term used in EU digital laws is "illegal content".[17]

In contrast, harmful content encompasses material that may not be illegal but is nonetheless considered detrimental to individuals or society — for example, disinformation, health misinformation, or content that undermines democratic processes. Addressing disinformation in a legal, regulatory or policy context requires a definition of the term to distinguish it from other types of content. Disinformation commonly refers to false or misleading information shared deliberately to deceive. Accordingly, it can be distinguished from misinformation, i.e. false information shared without intent to deceive or malinformation, which is true information used maliciously or out of context.[18] This category is particularly challenging to regulate, as much of it falls outside the scope of illegality, and it is thus often addressed under the broader notion of harmful content. Therefore, the scope of this report will extend beyond illegal content to disinformation as

[15] For a brief overview, see Ukrow J., "Introduction and Overview" in Cappello M. (ed.), *Media Law Enforcement without Frontiers*, IRIS *Special*, European Audiovisual Observatory, Strasbourg, 2018, pp. 3 et seq.
[16] *Netzwerkdurchsetzungsgesetz* (the Network Enforcement Act – NetzDG). The Act has been partly revoked by the implementing Act to the DSA.
[17] Illegal content is defined, for instance, in Article 3(h) DSA.
[18] For a definition of mis-, mal- and dis-information see Wardle, C. and Derakhshan, H., *Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making*, Council of Europe report DGI(2017)09, pp. 20 et seq.

a separate category, that is not necessarily encompassed under the notion “illegal” and poses distinct challenges for regulation.

In response to the scale, prevalence, and societal impact of illegal content and disinformation, a range of regulatory and governance models have evolved that seek to take account of the diversity of Internet intermediaries ranging from passive to active engagement and performing a variety of functions and services. The latter include social networking, blogging, messaging, discussion fora and bulletin boards, social news aggregation and rating platforms and video-sharing platforms, to name but a few. The focus here will be on platforms which as intermediaries host and disseminate content.

The first part of this publication addresses the legal framework of the Council of Europe before outlining the most important EU legal instruments governing Internet intermediaries. An Internet intermediary is broadly understood as an entity that facilitates the use of the Internet by providing services that enable communication, access to content, or the transmission and storage of data between users. Separate definitions for the notion as well as the services provided are encompassed in the various legal measures and will be outlined when necessary. Country examples focussing on different phenomena of illegal or harmful content and their responses under EU and national law seek to provide a snapshot of the variation in the enforcement of rules. A subsequent chapter will compare the variety of enforcement models. In the light of the legal background presented in the first part of this publication, as well as a brief presentation of the national legal frameworks for regulating online platforms in general, the country examples outline the specific rules on targeting the illegal or harmful content in question, and exemplify the application of said regime in a selected context. The concluding section will show how the report illustrates remaining and ongoing challenges when it comes to effectively tackling illegal and harmful content online.

2. The legal framework

2.1. The Council of Europe on content regulation and enforcement measures

Dr Sandra Schmitz-Berndt, Research Associate, Institute of European Media Law (EMR)

2.1.1. Enforcement measures and the fundamental rights framework in the Council of Europe

While "user-generated expressive activity on the Internet provides an unprecedented platform for the exercise of freedom of expression",[19] enforcing rules on specific content such as restricting access to, deleting or prosecuting certain speech *per se* interferes with the right to freedom of expression as guaranteed by Article 10 of the European Convention on Human Rights (ECHR).[20] The communication freedoms – freedom of information, freedom of expression and freedom of mass media communication – enshrined in Article 10(1) of the ECHR, as well as in comparable constitutional provisions, are a precondition for a functioning democracy. As rights to defend individuals against the state, the communication freedoms safeguard individual self-determination by shielding the communication process from state interference. Assessing whether such interference has occurred in a modern understanding of interference includes any state-imposed rule or action that constrains, obstructs, or renders wholly or partially impossible the exercise of behaviour protected by fundamental rights. In this sense, the enforcement of rules that affect communication can itself constitute an interference attributable to the state.[21]

However, the significance of communication rights goes beyond shielding individuals from arbitrary state interference. The European Court of Human Rights (ECtHR) has recognised that there can be additional inherent positive obligations for the effective respect of the rights concerned. Accordingly, in the view of the Court, the effective exercise of freedom of expression does not only depend on a state's duty not to interfere, but may also require positive measures of protection, even in the sphere of relations between

[19] *Delfi As v. Estonia* [GC] No. 64569/09 (ECtHR, 16 June 2015), paragraph 110.

[20] For an extensive overview with short summaries and quick accessibility of the cases see EAO, VERBO database, available here; previously also Voorhoof D. et al and McGonagle T. (Ed. Sup.), *Freedom of Expression, the Media and Journalists: Case-Law of the European Court of Human Rights*, IRIS *Themes,* European Audiovisual Observatory, Strasbourg 2024. For the framework for law enforcement at the level of national constitutional frameworks see Ukrow J., 'Framework for Law Enforcement against Online and Foreign Content Providers' in Cappello M. (ed.), *Media Law Enforcement without Frontiers,* IRIS *Special,* European Audiovisual Observatory, Strasbourg 2018.

[21] Mensching C., "Artikel 10 EMRK" in Karpenstein U. and Mayer F. C. (eds.), *Konvention zum Schutz der Menschenrechte und Grundfreiheiten: EMRK,* C.H.Beck München, 3rd ed., 2022, paragraph 27 with further references.

individuals.[22] Depending on the circumstances, private actors may also bear the indirect obligation to respect these rights with the obligation closely resembling or even matching those imposed on states. This becomes particularly relevant when private actors provide the basic infrastructure for public communication and assume roles that were traditionally considered public service tasks, such as the safeguarding of postal and telecommunications services.[23]

Article 10(2) of the ECHR sets out the possibility of limiting the exercise of the communication freedoms encompassed in Article 10(1) and the conditions under which such restrictions may be imposed; it also refers to a number of explicitly listed legitimate aims for interference by the ratifying state parties.

To date, the ECtHR has repeatedly recognised that the Internet provides an unprecedented platform for the exercise of freedom of expression.[24] Based on the Internet's accessibility and its capacity to store and communicate vast amounts of information, it is considered to play an important role in enhancing the public's access to news and facilitating the dissemination of information in general – including content that may be ignored by the traditional media.[25] At the same time, the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms, particularly the right to respect for private life, is considered higher than that posed by the press.[26] As a uniquely powerful communication tool, the ECtHR has acknowledged that the Internet is distinct from print media in its ability to store and transmit information globally and therefore requires tailored rules that reflect its technological features.[27] Furthermore, the important benefits of the Internet in, *inter alia*, the exercise of freedom of expression go hand-in-hand with a number of dangers, including the fact that clearly unlawful speech can be disseminated instantly on a global scale and may "remain persistently available online".[28] Further, it has been recognised by the Court that the risk of harm posed by content and communications on the Internet to the exercise and enjoyment of human rights and freedoms is certainly higher than that posed by the traditional press.[29]

As early as 2003, the Committee of Ministers of the Council of Europe adopted a declaration on freedom of communication on the Internet,[30] of which Principle 6 stipulated a limited liability of service providers for Internet content. Principle 6 foresees that in cases

---

[22] *Özgur Gündem v. Turkey*, No. 23144/93 (ECtHR, 16 March 2000), paragraph 43 with reference to *X and Y v. the Netherlands*, No. 8978/80 (ECtHR, 26 March 1985), paragraph 23.
[23] See BVerfG (Federal Constitutional Court), judgment of 22 February 2011, 1 BvR 699/06, paragraph 59.
[24] *Delfi As v. Estonia* [GC], No. 64569/09, paragraph 110; *Cengiz and others v. Turkey*, Nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015), paragraph 52; *Ahmet Yildirim v. Turkey*, No. 3111/10 (ECtHR, 18 December 2012), paragraph 48; *Times Newspapers Ltd (Nos. 1 & 2) v. the United Kingdom*, No. 3002/03 and 23676/03 (ECtHR, 10 March 2009), paragraph 27.
[25] *Ahmet Yildirim v. Turkey*, No. 3111/10, paragraph 48; as regards content not covered by the traditional press see: *Cengiz and others v. Turkey*, Nos. 48226/10 and 14027/11, paragraph 52.
[26] *Egill Einarsson v. Iceland*, No. 24703/15 (ECtHR, 7 February 2018), paragraph 46.
[27] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, No. 33014/05 (ECtHR, 5 May 2011), paragraph 63.
[28] *Delfi As v. Estonia* [GC], No. 64569/09, paragraph 110.
[29] *Editorial Board of Pravoye Delo and Shtekel v. Ukraine*, No. 33014/05, paragraph 63.
[30] Council of Europe, Committee of Ministers, Declaration on freedom of communication on the Internet, Decl(28/05/2003).

where the functions of the service providers are wider and they store content emanating from other parties, states may hold them co-responsible if they do not act expeditiously to remove or disable access to information or services as soon as they become aware, as defined by national law, of their illegal nature or, in the event of a claim for damages, of facts or circumstances revealing the illegality of the activity or information. The Council of Europe thereby replicated the liability concept applicable under national law in EU member states based on Article 14 of the EU e-Commerce Directive.[31]

Subsequently, the Council of Europe has over many years addressed – directly or indirectly – the enforcement of rules on illegal content and disinformation online in numerous further policy documents, including recommendations and declarations. These political standard-setting texts are – in contrast to the Council of Europe's conventions for signatories – not legally binding but serve to support the interpretation of the conventions including the ECHR by applying general principles to sample scenarios or specific contexts and by setting out a differentiated and graduated response.[32]

In the preamble to its rule of law-based policy instrument Recommendation CM/Rec(2018)2 on the roles and responsibilities of Internet intermediaries, the Committee of Ministers further observes that "a wide, diverse and rapidly evolving range of players, commonly referred to as 'Internet intermediaries', facilitate interactions on the Internet between natural and legal persons by offering and performing a variety of functions and services".[33] "Owing to the multiple roles intermediaries play, their corresponding duties and responsibilities and their protection under law should be determined with respect to the specific services and functions that are performed".[34] Accordingly, with the evolving diverse roles of online actors, the Council of Europe has moved away from the term "Internet service provider", commonly used for access, caching or host providers, in favour of the broader designation of "Internet intermediaries". Addressing the obligations of states and the responsibilities of Internet intermediaries, the Appendix to Recommendation CM/Rec(2018)2 sets out guidelines for states on actions to be taken vis-à-vis Internet intermediaries. The obligations of states with respect to the protection and promotion of human rights and fundamental freedoms in the digital environment include taking into account the substantial differences in the size, nature, function and organisational structure of intermediaries when devising, interpreting and applying the legislative framework.[35] The Committee of Ministers acknowledges that platform providers may play different roles in content production and dissemination processes, for instance by managing or curating the content or playing an editorial role, thus requiring a graduated or differentiated approach.[36]

---

[31] European Union, "Directive on electronic commerce", 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 178/1, 17 July 2000.

[32] This approach has been suggested in the Council of Europe's Recommendation CM/Rec(2011) on a new notion of media. See: Recommendation CM/Rec(2011)7 – Recommendation of the Committee of Ministers to member states on a new notion of media.

[33] Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of Internet intermediaries, Preamble, paragraph 4.

[34] Ibid, paragraph 11.

[35] Council of Europe, Appendix to Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of Internet intermediaries, paragraph 1.1.5.

[36] Ibid, paragraph 1.3.9.

According to Recommendation CM/Rec(2011)7, this approach requires that each actor whose services are identified as media or as an intermediary or auxiliary activity should benefit from both the appropriate form (differentiated) and the appropriate level (graduated) of protection and that responsibility should be delimited.[37]

States should ensure that legislation, regulation and policies relating to Internet intermediaries are effectively implementable and enforceable and do not unduly restrict the operation and free flow of transborder communication.[38] The Appendix to Recommendation CM/Rec(2018)2 clarifies that any measure by public authorities addressed to Internet intermediaries to restrict access, including the blocking or removal of content, or any other measures that could lead to a restriction of the right to freedom of expression must pass the three-step test of Article 10 ECHR. This means that any request, demand or other action by public authorities addressed to Internet intermediaries to restrict access (including the blocking or removal of content) shall be prescribed by law, pursue one of the legitimate aims foreseen in Article 10 of the ECHR, be necessary in a democratic society and be proportionate to the aim pursued.[39] Nevertheless, in the context of these measures, state authorities should seek an order by a judicial authority or other independent administrative authority, whose decisions are subject to judicial review, before requiring intermediaries to restrict access to content except in cases involving inherently illegal material such as content involving child sexual abuse material, or where urgent action is justified under the conditions prescribed in Article 10 of the ECHR.[40]

Furthermore, Recommendation CM/Rec(2018)2 advises states to refrain from requiring intermediaries to monitor content they merely give access to, or transmit or store. Any request to intermediaries or co-regulatory initiatives must avoid a general monitoring obligation.[41] Recommendation CM/Rec(2018)2 also addresses responsibility for third-party content, noting that intermediaries should not be held liable for content which they merely give access to or which they transmit or store, whereas co-responsibility may be established for stored content if intermediaries do not act expeditiously to restrict access to content or services as soon as they become aware of their illegal nature, including through notice-based procedures.[42]

As regards notification procedures, Recommendation CM/Rec(2018)2 notes that these should not be designed in a manner that incentivises the takedown of legal content, for instance via inappropriately short timeframes, and that they should contain the information necessary to allow intermediaries to take appropriate action.[43] In light of the human rights-centred approach of the Council of Europe's policy measures, any interference by intermediaries with the free and open flow of information and ideas, must be limited to

[37] Appendix to Council of Europe Recommendation CM/Rec(2011)7 of the Committee of Ministers to member states on a new notion of media, Criteria for identifying media and guidance for a graduated and differentiated response, paragraph 7.
[38] Council of Europe, Recommendation CM/Rec(2018)2 of the Committee of Ministers to member states on the roles and responsibilities of Internet intermediaries, paragraph 1.1.6.
[39] Ibid, paragraph 1.3.1.
[40] Ibid, paragraph 1.3.2.
[41] Ibid, paragraph 1.3.5.
[42] Ibid, paragraph 1.3.7.
[43] Ibid.

specific legitimate purposes and respect principles of transparency and accountability as well as providing for access to an effective remedy.[44] However, this does not prevent states from imposing obligations upon intermediaries to mitigate online risks and respond to the dissemination of illegal content by introducing, for instance, content moderation mechanisms. Subsequent recommendations concerned the impact of digital technologies on freedom of expression,[45] the human rights impact of algorithmic systems[46] and combatting hate speech.[47] In an overarching approach, Recommendation CM/Rec(2022)11 on principles for media and communication governance[48] addresses the risks caused by platforms disseminating illegal and harmful content, explicitly referring to risk-based and human rights compliant content moderation as an appropriate response.

Recommendation CM/Rec(2022)13 on the impacts of digital technologies on freedom of expression[49] is a further effort to ensure that digital technologies serve rather than curtail the rights enshrined in Article 10 of the ECHR. In terms of accountability and redress, this recommendation requires states to ensure effective redress mechanisms against restrictions on free speech.[50] When Internet intermediaries enforce restrictions on freedom of expression, they should provide directly or indirectly affected users with clear information on the regulation under which their rights have been limited. Intermediaries should also provide timely and effective redress mechanisms.[51]

Considering that defamatory and other types of unlawful speech can be disseminated "like never before, worldwide, in a matter of seconds, and sometimes remain persistently available online" and that the rights under Articles 10 and 8 of the ECHR "deserve equal respect", "the possibility of imposing liability for defamatory or other types of unlawful speech must, in principle, be retained, constituting an effective remedy for violations of personality rights".[52] Speech that is incompatible with the values proclaimed and guaranteed by the ECHR is not protected by Article 10 of the ECHR by virtue of Article 17 of the ECHR, which prohibits the abuse of rights. Although there is a substantial body of case law on how to conduct the balancing exercise between Articles 10 and 8 of the ECHR, the Council of Europe considered it necessary to address the specificities of hate speech and in particular such speech in an online context in a separate Recommendation on combatting hate speech.[53] Said Recommendation CM/Rec(2022)16 provides guidance for states to implement a comprehensive and calibrated set of legal and non-legal measures.

---

[44] Ibid, paragraphs 2.2 *et seq*.
[45] Council of Europe, Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impact of digital technologies on freedom of expression.
[46] Council of Europe, Recommendation CM/Rec(2020)1 of the Committee of Ministers to member States on the human rights impact of algorithmic systems.
[47] Council of Europe, Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combatting hate speech.
[48] Council of Europe, Recommendation CM/Rec(2022)11 of the Committee of Ministers to member States on principles for media and communication governance.
[49] Council of Europe, Recommendation CM/Rec(2022)13 of the Committee of Ministers to member States on the impacts of digital technologies on freedom of expression.
[50] Ibid, Appendix, paragraph 4.1.
[51] Ibid, paragraph 4.5.
[52] *Delfi As v. Estonia* [GC], No. 64569/09, paragraph 110.
[53] Council of Europe, Recommendation CM/Rec(2022)16 of the Committee of Ministers to member States on combatting hate speech.

While the general principles applicable to offline publications also apply online, Recommendation CM/Rec(2022)16 pays special attention to the online environment in which most of today's hate speech can be found. In view of the continuing victimisation that occurs when such content remains online, the recommendation calls upon member states to focus on removing online hate speech alongside criminal investigations.[54]

Considering that online hate speech spreads over national borders, Recommendation CM/Rec(2022)16 recognises the need for harmonisation to prevent and combat hate speech in an effective way.[55] In line with Recommendation CM/Rec(2018)2, this harmonisation needs to address the roles and responsibilities of all stakeholders including Internet intermediaries.[56]

Recommendation CM/Rec(2022)16 requires removal procedures, including the conditions for removal, as well as the responsibilities imposed upon intermediaries to be transparent, clear and predictable and to provide for redress mechanisms.[57] Due to the likely anonymity of the perpetrator, states need to provide for a system for the disclosure of subscriber information from service providers.[58] Further, the recommendation addresses content moderation, which in view of the use of artificial intelligence (AI), should be overseen by human moderators.[59] Besides appointing a sufficient number of trained content moderators, Recommendation CM/Rec(2022)16 encourages collaborative models such as trusted flaggers and fact-checkers and cooperation with civil society organisations that work on hate speech.[60] The recommendations have been complemented by the Council of Europe's Guidance Notes on content moderation (2021),[61] and on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner (2023).[62]

Most recently, the Parliamentary Assembly of the Council of Europe's (PACE) Resolution 2590[63] of January 2025 on regulating content moderation on social media to safeguard freedom of expression restates that social media providers are legally obliged to remove any illegal content once aware of its existence, as well as noting that it is "incumbent upon social media to combat the dissemination of harmful content".[64] As bearers of fundamental rights, such as the right to property and freedom of enterprise, as well as to draft terms and conditions with a contractual character (where users are bound by them on a take-it-or-leave-it basis), social media companies can determine how users

[54] Ibid, Preamble.
[55] Ibid, paragraph 16.
[56] Ibid, paragraph 17.
[57] Ibid., paragraph 20.
[58] Ibid, paragraph 24.
[59] Ibid., paragraph 33.
[60] Ibid., paragraphs 34 *et seq*.
[61] Council of Europe, Steering Committee for Media and Information Society, Guidance Note on content moderation, 2021.
[62] Council of Europe, Steering Committee for Media and Information Society, Guidance Note on countering the spread of online mis- and disinformation through fact-checking and platform design solutions in a human rights compliant manner, 2024.
[63] Council of Europe, Parliamentary Assembly, Regulating Content Moderation on Social Media to Safeguard Freedom of Expression, PACE Resolution 2590.
[64] Ibid, paragraph 2.

can use their services and what content they can post. Also, they can set up internal content moderation policies enabling them to demote, restrict access to, or remove content, and to suspend or terminate user accounts.[65] Considering their global reach and private contractual power including content moderation policies and commercial or ideological decisions about content, social media providers may have immense influence on public opinion. Recognising the power imbalance and the need to combat the dissemination of harmful content, PACE emphasises the necessity for states to establish a regulatory corrective framework for content moderation that balances content moderation with the protection of freedom of expression.[66] Resolution 2590 calls on both member states and social media platform providers to implement content moderation systems that ensure transparency, access, oversight and redress mechanisms and provide for restraint being applied especially when content is legal or of public interest.[67]

In content moderation but also in other instances of content placing, providers increasingly rely on algorithmic systems including AI. On 17 May 2024, the Council of Europe adopted the first ever internationally legally binding treaty for signatory states for the use of AI with its Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law.[68] States are encouraged to ensure that legislation governing AI systems guarantees transparency and accountability, while upholding the principles of democracy and providing for effective oversight and the consistent review of these systems.[69]

While all the previously mentioned recommendations establish safeguards to protect freedom of expression, the Council of Europe's framework – as a fundamental rights framework – does not prescribe specific enforcement mechanisms. The following sections therefore examine relevant case law of the ECtHR, grouped in thematic blocks exemplifying the graduated response system.

2.1.2. Internet intermediaries and other online actors as addressees of enforcement measures

As already mentioned above and as emphasised by the ECtHR, the Internet plays an important role "for the exercise of the right to freedom of expression generally".[70] While the original perpetrators of illegal content are most naturally the primary target for

[65] Ibid, paragraph 3.
[66] Ibid, paragraphs 4 *et seq*.
[67] Ibid, paragraphs 10 *et seq*.
[68] Council of Europe, Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law (CETS No. 225), 2024. Details on the status of signatories and entry into force can be found at *here*.
[69] For an overview of the guiding principles of AI regulation see Cole M.D., "AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments" in *Journal of AI and Regulation*, 1(1), 2024, pp. 126-142; on the Framework Convention, see Gartner M., "Council of Europe: States Adopt First Binding Framework Treaty on AI" in *Journal of AI and Regulation*, 1(3), 2024, pp. 342-349.
[70] *Times Newspapers Ltd (Nos. 1 & 2) v. the United Kingdom*, Nos. 3002/03 and 23676/03, paragraph 27.

enforcement action,[71] Internet intermediaries as the conveyers of content have also been subject to enforcement measures early on. One of the reasons for this is that they are easier to identify while at the same time having the means to restrict access to or delete illegal content. With a diversification of the roles of intermediaries from more passive conduits or hosts to active roles in content production and dissemination processes, for instance by managing or curating the content or playing an editorial role, case law is also evolving. The graduated approach reflected in recommendations of the Committee of Ministers is mirrored in the case law of the ECtHR which addresses Internet intermediaries in light of their rights, duties and responsibilities.

2.1.2.1. Duties and responsibilities of Internet intermediaries regarding unlawful third-party content

The objective liability of Internet portals for content emanating from third parties is considered incompatible with Article 10 of the ECHR.[72] Even in the case of civil law measures, the attribution of liability for third-party comments may have negative consequences, for example for the comment area of an online portal and may have a chilling effect on freedom of expression on the Internet.[73] This can be especially detrimental for non-commercial websites.[74] In cases involving criminal liability – where responses must be adapted and proportionate to the seriousness of the content in question – such repercussions on freedom of expression may therefore be considered potentially heightened.[75]

In cases of unlawful third-party user comments, the rights and interests of others and of society as a whole may, however, entitle states to impose liability on Internet intermediaries without contravening Article 10 of the ECHR if they failed to take measures to remove clearly unlawful comments without delay, even in cases where there had not been a notice by the alleged victim or from third parties.

In the landmark case of *Delfi AS v. Estonia*, the ECtHR discussed for the first time the civil responsibility and duty of care of a professional host provider as regards defamatory speech.[76] Although the large online news portal operated by Delfi AS had an automated filtering system and a notice-and-takedown procedure in place, Estonian courts established liability for unlawful third-party comments posted on the portal's website in response to one of its own articles.

---

[71] On the liability of the original authors of a comment, see *Delfi As v. Estonia* [GC], No. 64569/09, paragraphs 147 *et seq*.

[72] *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13 (ECtHR, 2 February 2016), paragraph 91.

[73] *Sanchez v. France [GC]*, op. cit., paragraph 205 with reference to *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 86.

[74] *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 86.

[75] *Sanchez v. France [GC]*, op. cit., paragraph 206.

[76] For a case comment, see Korpisaari P., "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", in *Journal of Media Law,* 14(2), 2022, pp. 352-377.

In consideration of the particular nature of the Internet, the ECtHR recognised that the "duties and responsibilities" of an online news portal for the purposes of Article 10 of the ECHR may differ to some degree from those of a traditional publisher as regards third-party content.[77] Although Internet news portals are not publishers of third-party content in the traditional sense, they may be held responsible for it under certain circumstances.[78] The distinction between how third-party content is treated for Internet news portals versus traditional publishers aligns with international standards, which increasingly recognise the need to apply different legal principles to traditional media and online news portals on which third-party content is typically disseminated without editorial control being part of the publishing process.[79]

In order to assess whether an Internet portal operator becomes liable for third-party content, the ECtHR has identified four criteria that seek to ensure that a fair balance is struck between the competing interests – the right to freedom of expression and the right to reputation of another person or entity.[80]

These criteria, applicable in cases of civil, criminal and administrative liability, are (1) the context of the comments, (2) the liability of the authors of the comments, (3) the measures taken by the applicants and the conduct of the aggrieved party, and (4) the consequences of the domestic proceedings for the applicants.

Consideration of the context and content of the impugned comments is required to determine the overall lawfulness of third-party content, that is, whether the permissible limits of freedom of expression are exceeded while paying regard to the immediate context and the specificities of the style of communication on certain Internet portals.[81] For instance, the impact of racist and xenophobic discourse becomes greater and more harmful in an election context and where the political and social climate is troubled.[82]

In the case of *Delfi AS v. Estonia* the assessment of the context extended to the professional and commercial character of the news platform.[83] In view of the commercial nature of seeking to attract a large number of comments, the Court noted that Delfi had to be distinguished from

> *other fora on the Internet where third-party comments can be disseminated, for example, an Internet discussion forum or a bulletin board where users can freely set out their ideas on any topics without the discussion being channelled by any input from the forum's manager;*

[77] *Delfi As v. Estonia [GC]*, op. cit. paragraph 113; see also *Orlovskaya Iskra v. Russia*, No. 42911/08 (ECtHR, 21 February 2017), paragraph 109.
[78] *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 62.
[79] See *Delfi As v. Estonia [GC]*, paragraphs 112 *et seq*.
[80] Ibid, paragraphs 142 *et seq*.; *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 61.
[81] *Sanchez v. France [GC]*, op. cit., paragraphs 174 *et seq*.; *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 77.
[82] *Sanchez v. France [GC]*, paragraph 176.
[83] *Delfi As v. Estonia [GC]*, paragraph 144.

or a social media platform where the platform provider does not offer any content and where the content provider may be a private person running the website or a blog as a hobby.[84]

While professional entities which create social networks and make them available to other users necessarily have certain obligations, a Facebook account holder only falls in the category of "other fora on the Internet where third-party comments can be disseminated" for the provision of their Facebook "wall".[85] This does not release the account holder or any other provider from duties and responsibilities in terms of third-party content because an exclusion of liability might facilitate or even encourage abuse and misuse including hate speech and disinformation.[86]

The attribution of liability for third-party comments depends on the measures taken and the conduct of the aggrieved party.[87] The measures required vary depending on the moderation or vetting techniques available and must be examined carefully to avoid a chilling effect on freedom of expression.[88] In any case the competing interests must be balanced.[89] Imposing civil liability on an Internet news portal for refusing or failing to remove clearly unlawful content as in the *Delfi AS v. Estonia* case can be justified even without notice from the injured party or from third parties,[90] meaning that some form of monitoring would be necessary, especially where content is likely to provoke heated discussions.[91] In fact, the ECtHR considers it largely uncontroversial that a minimum degree of subsequent moderation or automated filtering is desirable to swiftly identify and remove clearly unlawful comments ideally within a reasonable time, even in the absence of a notification from an injured party.[92]

2.1.2.2. Duties and responsibilities of non-professional entities for unlawful third-party content

The responsibility discussed above may lie either with the host platform, acting as a professional provider, or with account holders, who publish their own content and permit others to comment on it.[93] In the case *of Sanchez v. France*, the ECtHR assessed the extent to which the liability regime for host platforms can be applied to the account holder of a Facebook page when third parties post unlawful comments on their wall. In this scenario,

[84] Ibid, paragraph 116.
[85] *Sanchez v. France [GC]*, op. cit., paragraph 180.
[86] Ibid, paragraph 185.
[87] For an overview of what can be expected from host platform providers see Korpisaari P., "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", in *Journal of Media Law,* 14(2), 2022, pp. 352-377.
[88] See *Sanchez v. France [GC]*, paragraph 182.
[89] *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 88.
[90] Ibid, paragraph 91 referring to *Delfi As v. Estonia* [GC], No. 64569/09, paragraph 157. See also Enarsson T., "Navigating hate speech and content moderation under the DSA: Insights from ECtHR case law", in *Information & Communications Technology Law*, 33(3), 2024, pp. 384-401, 392 *et seq*.
[91] See *Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary*, No. 22947/13, paragraph 73.
[92] *Sanchez v. France [GC]*, paragraph 190.
[93] Ibid.

the ECtHR acknowledged that prior content moderation is practically impossible – technically, but also resource-wise if the account is used for non-commercial purposes and is very popular.[94]

A criminal conviction for failing to remove third-party content under national law, where the account holder of a Facebook wall is deemed to have assumed the role of a content producer, does not constitute a violation of Article 10 of the ECHR if the account holder failed to respect certain duties and responsibilities. Factual elements to be taken into account include the personal capacity of the account holder, or more generally the intermediary; for instance, a politician using their social media account for political purposes and who is experienced in public communication must be aware of the heightened risk that excessive or immoderate remarks may appear in response to a post made during election time and reach a wider audience.[95] Changing the privacy settings can be a mitigating measure to decrease visibility or limit who can post a response to a post. Where awareness of the issues raised by some comments can be established, a minimal verification can be expected.[96] The latter applies in particular where the social media account is consulted on a daily basis and specific users respond to and complement each other in a conversation following an initial post and where that conversation content has been notified as unlawful.[97] While in the case of *Sanchez v. France* the criminal conviction of the Facebook account holder for third-party comments did not amount to a violation of Article 10 of the ECHR, the threshold to establish "awareness" of unlawful content is highly controversial as indicated by the concurring[98] and dissenting opinions[99] in the *Sanchez v. France* case.[100]

In line with the standards on international law, liability can be avoided if unlawful content is removed "without delay" once the intermediary becomes aware of the illegality of the content.[101]

2.1.2.3. Duties and responsibilities of creators of hyperlinks

Similar to the objective liability of Internet portals for content emanating from third parties, imposing objective liability for hyperlinks is incompatible with Article 10 of the ECHR. Hyperlinks can be distinguished from traditional acts of publication because they merely direct users to content available elsewhere on the Internet and are not a separate act of

[94] Ibid, paragraph 185.
[95] Ibid, paragraphs 186 *et seq*.
[96] Ibid, paragraph 194.
[97] Ibid, paragraphs 199 *et seq*.
[98] Ibid, Concurring Opinion of Judge Küris.
[99] Ibid, Dissenting Opinion of Judge Ravarani; Dissenting Opinion of Judge Bosnjak; Joint Dissenting Opinion of Judges Wojtyczek and Zünd.
[100] See also Husovec M. et al., "Grand confusion after *Sanchez v. France*: Seven reasons for concern about Strasbourg jurisprudence on intermediaries", in *Maastricht Journal of European and Comparative Law*, 31(3), 2024, pp. 385-411.
[101] *Delfi As v. Estonia [GC]*, op. cit., paragraph 153.

communication.[102] Their purpose is to allow users to navigate to and from material in a network characterised by the availability of an immense amount of information.[103] Further, the person referring to information via a hyperlink does not exercise control over the content to which access is enabled and which may change after the creation of the link.[104]

Due to these particularities, sufficient and relevant grounds are necessary to establish liability of the creator of a hyperlink, requiring a careful assessment of the "duties and responsibilities" of the link creator. The following questions need to be examined: whether the creator (1) had endorsed the impugned content; (2) had repeated the impugned content (without endorsing it); (3) had merely put a hyperlink to the impugned content (without endorsing or repeating it); (4) had known or could reasonably have known that the impugned content was defamatory or otherwise unlawful; (5) had acted in good faith, respected the ethics of journalism and performed the due diligence expected in responsible journalism.[105]

In that context it must be noted that a general requirement for journalists to systematically and formally distance themselves from the content of a quotation that might insult or provoke others or damage their reputation is not reconcilable with the role of the press in providing information on current events, opinions and ideas.[106]

The same reasoning has subsequently been applied to the sharing of third-party content online through social media platforms noting that the act of sharing certain content is a common means of communication and social interaction, and could contribute to an informed citizenry.[107] However, where material is taken out of its context without further comments and could be reasonably perceived as stirring up ethnic discord or violence, liability for making third-party content available for access can be justified.[108]

2.1.3. The scope of enforcement measures

While content moderation rules included in the terms and conditions of social media platforms may also foresee the suspension or termination of a user's account,[109] the ECtHR has set limits on state-imposed enforcement measures in a number of judgments. While

[102] *Magyar Jeti Zrt v. Hungary*, No. 11257/16 (ECtHR, 4 December 2018), paragraph 74. This issue has previously been discussed by the CJEU in relation to the concept "communication to the public" within the meaning of Article 3(1) of Directive 2001/29/EC on the harmonisation of certain aspects of copyright and related rights in the information society, see C-466/12 *Svensson and Others v. Retriever Sverige AB* (CJEU, 13 February 2014), ECLI:EU:C:2014:76, paragraphs 18 *et seq*.
[103] *Magyar Jeti Zrt v. Hungary*, No. 11257/16, paragraph 73.
[104] Ibid, paragraph 75.
[105] Ibid, paragraph 77.
[106] Ibid, paragraph 80 with reference to *Thoma v. Luxembourg*, No. 38432/97 (ECtHR, 29 March 2001), paragraph 64. A similar question is currently pending before the CJEU in a request for a preliminary ruling from the Budapest Regional Court (C-843/24 *24.hu*).
[107] *Kilin v. Russia*, No. 10271/12 (ECtHR, 11 May 2021), paragraph 79.
[108] Ibid, paragraphs 87 *et seq*.
[109] Council of Europe, Parliamentary Assembly, Regulating Content Moderation on Social Media to Safeguard Freedom of Expression (PACE Resolution 2590, paragraph 3), 2025.

the deletion or blocking of access to a certain piece of illegal content is likely to pass the three-step test of Article 10 of the ECHR, any measure that goes further than targeting the illegal content as such and interferes with lawful content is unlikely to satisfy the requirement of foreseeability and likely to fail the proportionality test.

2.1.3.1. Blocking access to websites

The ECtHR has had to deal with measures taken by national authorities to block access to certain Internet sites on multiple occasions. A blanket website blocking of YouTube resulted in undue interference with the rights of users — who were not directly targeted by the measure — to receive and impart information or ideas; as a result, these users were entitled to invoke this right before the Court.[110] In this case, the way national court decisions concerning specific content had to be implemented resulted in any access to the entire website being blocked.[111] The unique nature of the platform concerned and the potential impact of rendering large quantities of information inaccessible was held to substantially restrict the rights of users and to have a significant collateral effect.[112]

In contrast, the mere fact that users had been indirectly affected by a blocking measure against two music-sharing websites was not sufficient to claim "victim status" under Article 34 of the ECHR and consequently did not give users of that service standing to bring the case before the ECtHR.[113] Blocking access to an Internet site may also result in the blocking of another website with the same IP address, and, despite substantially restricting the rights of Internet users, will be unlikely to satisfy the foreseeability requirement under the ECHR.[114]

In cases of prior restraint, a legal framework is required, ensuring both tight control over the scope of bans and effective judicial review to prevent any abuse of power.[115] The judicial review of a blocking measure, based on a weighing-up of the competing interests at stake and designed to strike a balance between them, is inconceivable without a framework establishing precise and specific rules regarding the application of preventive restrictions on freedom of expression.[116] In cases concerning prior restraints on publications calling for participation in a public event, it must be possible to obtain a judicial review of the blocking measure before the date of the public event in question so that the review does not become meaningless.[117]

---

[110] Cengiz and others v. Turkey, Nos. 48226/10 and 14027/11, paragraphs 52 *et seq*. and *Ahmet Yildirim v. Turkey*, No. 3111/10, paragraphs 49 *et seq*.
[111] *Ahmet Yildirim v. Turkey*, No. 3111/10, paragraph 66.
[112] Ibid; *Cengiz and others v. Turkey*, Nos. 48226/10 and 14027/11, paragraph 64.
[113] *Akdeniz and Others v. Turkey*, Nos. 41139/15 and 41146/15 (ECtHR, 4 May 2021), paragraph 24.
[114] *Vladimir Kharitonov v. Russia*, No. 10795/14 (ECtHR, 23 June 2020), paragraphs 45 *et seq*. The key problem with IP address blocking is that many addresses are shared between multiple content providers (shared webhosting). If a particular IP address is blocked, then all of the web content under that particular IP address will become inaccessible.
[115] *Kablis v. Russia*, Nos. 48310/16 and 59663/17 (ECtHR 30 April 2019), paragraph 92.
[116] *Ahmet Yildirim v. Turkey*, No. 3111/10, paragraph 64.
[117] *Kablis v. Russia*, Nos. 48310/16 and 59663/17, paragraphs 85 *et seq*.

A full-scale blocking order against a website is regarded to be an extreme measure which the ECtHR has compared to banning a newspaper or broadcaster.[118] Accordingly, the unjustified complete blocking of media outlets, which ignores the distinction between illegal and legal content, has been considered arbitrary and manifestly unreasonable.[119] The same applies if the blocking is upheld even though the material deemed illegal had been removed.[120]

Furthermore, it must be ensured that any blocking is proportionate to the aim pursued. As noted above, rules on illegal content and the respective enforcement measures must be narrowly tailored. Any blocking measure should strictly target the unlawful content and avoid arbitrary or excessive effects. Accordingly, it can be concluded that blanket blocking orders are unlikely to be compliant with Article 10 of the ECHR; authorities need to assess whether less intrusive alternatives, such as the removal of specific posts, could achieve the same objective without disproportionately limiting access to lawful expression. In particular, the impact on third parties and the chilling effect on online speech must be considered.

2.1.3.2. Blocking of social media accounts

The blocking of social media accounts was addressed in the case of *Kablis v. Russia*, where, *inter alia*, a social media account was blocked to prevent breaches of the law in the sphere of distribution of information as well as to maintain public order. First, the ECtHR found that the possibility for the individual concerned to simply create a new social media account was irrelevant to the assessment of whether the interference was justified.[121] Since any interference with freedom of expression must be necessary in a democratic society, it must meet a pressing social need and the authorities must provide relevant and sufficient reasons for the restriction. Such a reason could be, for example, that the social media account posed a risk to public safety or was likely to lead to public disorder or crime.[122] Similar to the blocking of an entire website or webpage, Article 10 of the ECHR requires that authorities take into account, among other aspects, the fact that blocking an entire social media account renders large quantities of information inaccessible. Such a measure substantially restricts the rights of Internet users and has a significant collateral effect on the material that has not been found to be illegal.[123] Careful scrutiny is therefore essential to ensure that any such restriction is proportionate to the legitimate aim pursued.

[118] *OOO Flavus and Others v. Russia, Nos. 12468/15, 23489/15, and 19074/16* (ECtHR, 23 June 2020), paragraph 37 and *Bulgakov v. Russia*, No. 20159/15 (ECtHR, 23 June 2020), paragraph 34 with further references.
[119] *OOO Flavus and Others v. Russia*, paragraph 34; *Bulgakov v. Russia*, No. 20159/15, paragraph 34.
[120] *Bulgakov v. Russia*, No. 20159/15, paragraphs 34 *et seq*.
[121] *Kablis v. Russia*, No. 48310/16 and 59663/17, paragraph 84.
[122] Ibid, paragraph 88.
[123] Ibid, paragraph 94 with reference to *Ahmet Yildirim v. Turkey*, No. 3111/10, paragraph 66, and *Cengiz and others v. Turkey*, Nos. 48226/10 and 14027/11, paragraph 64.

2.2. The European Union legal framework on content regulation and enforcement measures

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

2.2.1. Enforcement measures in light of primary EU law

Having addressed the limits that Article 10 of the ECHR imposes on enforcement measures by the states parties to the ECHR, it is also necessary to turn to the specific challenges posed by enforcement within the framework of EU primary law.[124] While fundamental rights provide essential boundaries for state action, the effective implementation of content regulation — particularly in the digital environment — must also be assessed in light of EU constitutional principles, such as the allocation of competences,[125] the internal market freedoms, the common values and the principle of sincere cooperation under Article 4(3) of the Treaty on European Union (TEU).[126] These dimensions raise complex questions about how enforcement measures can be coordinated across member states.

In essence, when it comes to the internal market and the relationship between EU member states as well as with institutions at an EU level, two key aspects come into play. First, the EU legal framework provides specific rules for dispute settlement. Second, interactions between member states are shaped by principles such as the "country of origin principle",[127] which is prominently featured in EU law and a cornerstone of the internal market, particularly through the case law of the Court of Justice of the European Union (CJEU).[128] Under this principle, an economic operator established in one member state is required to comply with the legal rules of its country of origin, but is not subject to additional legal obligations in the member state(s) where its goods or services are offered

[124] See in that regard also Ukrow J., 'Framework for Law Enforcement against Online and Foreign Content Providers' *in* Capello M. (ed.), *Media Law Enforcement without Frontiers,* IRIS *Special,* European Audiovisual Observatory, Strasboug 2018.

[125] See Cole, M.D., Ukrow J. and Etteldorf C., *On the Allocation of Competences between the European Union and its Member States in the Media Sector*, Nomos, Baden-Baden, 2021.

[126] Treaty on European Union in its consolidated version, 15 March 2025.

[127] For a general discussion of the country-of-origin principle, see, for example, Cole M.D., "The Country of Origin Principle – From State Sovereignty under Public International Law to Inclusion in the Audiovisual Media Services Directive of the European Union" *in* Meng W., Ress G. and Stein T. (eds.), *Europäische Integration und Globalisierung – Festschrift zum 60-jährigen Bestehen des Europa-Instituts*, Nomos, Baden-Baden, 2011, pp. 113-130; Cole M.D., Etteldorf C. and Ullrich C., *Updating the Rules for Online Content Dissemination*, Bd. 83 Schriftenreihe Medienforschung der LfM NRW, Nomos, Baden-Baden, 2021, pp. 143 *et seq*.; Rowland D., Kohl U. and Charlesworth A., *Information Technology Law*, Routledge, Abingdon, 5th ed. 2017, pp. 268 *et seq*.; Schilling K., *Binnenmarktkollisionsrecht*, De Gruyter, Berlin, 2006, pp. 74 *et seq*.; Garabiol-Furet M.-D., "Plaidoyer pour le principe du pays d'origine" *Revue du Marché commun et de l'Union Européenne*, 2006, pp. 82-87.

[128] C-376/22 *Google Ireland v. KommAustria* [2023] ECLI:EU:C:2023:835; C-665/22 *Amazon Services Europe v. AGCOM* [2024] ECLI:EU:C:2024:435; Joined Cases C-664/22 and C-666/22 Google Ireland and Others v. AGCOM [2024] ECLI:EU:C:2024:434; C-663/22 Expedia Inc. v. AGCOM [2024] ECLI:EU:C:2024:433; Joined Cases C-662/22 and C-667/22 AirBnB and others v. AGCOM [2024] ECLI:EU:C:2024:432.

or can be received, meaning that no additional requirements should be imposed other than those in the place of establishment. This approach reduces financial, administrative, and staffing burdens, and prevents duplicative checks or requirements that would otherwise hinder cross-border economic activity.

Responsibility for assessing the legality of a service consequently lies primarily with the member state of origin. The ability to choose the country of origin is rooted in the freedom of establishment, which allows companies and self-employed individuals to freely choose the location of their establishment within the EU. However, the limitation on member states' ability to take action against foreign service providers applies only within the scope of the free movement of services when the provider is established in another member state or in a third state that is a party to the European Economic Area (EEA) Agreement. In contrast, providers not established in an EU/EEA member state are subject to the general rules of public international law. In addition, secondary law can foresee further specific derogation possibilities from the country of origin principle. Targeted member states or those where a service by a provider established in another member state is ultimately received may intervene exceptionally — specifically, where a justified and proportionate restriction on the free movement of services is warranted. This may be based on either explicit or implicit grounds recognised under EU law, such as public policy,[129] public security, or the protection of consumers. Any such ground is interpreted strictly by the CJEU.[130]

Where secondary legislation concretely defines the scope of the fundamental freedoms, such harmonising rules must take precedence in the legal assessment. Key elements of relevance in the context of this publication include the Audiovisual Media Services Directive (AVMSD)[131] and the e-Commerce Directive (ECD),[132] which provide sector-specific rules governing the cross-border provision of services in the internal market.

[129] See C-376/22 *Google Ireland v. KommAustria*.

[130] See emphasis made by Advocate General Szpunar in his Opinion in Case *C-376/22 Google Ireland v. KommAustria* [2023] ECLI:EU:C:2023:467, paragraph 64.

[131] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (AVMSD), OJ L 95/1, last amended by 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 - AVMSD) in view of changing market realities, OJ L 303, 28 November 2018, as well as by Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L 2024/1083, 17 April 2024.

[132] 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 July 2000.

2.2.2. European Union secondary law on content regulation and enforcement measures

2.2.2.1. Regulating media and VSPs: the AVMSD and the EMFA

The AVMSD sets out the legal framework in accordance with which action against cross-border providers of linear television, on-demand video services and video-sharing platforms (VSPs) may be taken by the member states in the material area coordinated by its provisions – especially audiovisual commercial communication, the protection of minors and combatting incitement to hatred. Being a directive, member states have to transpose the provisions into national law, meaning, for instance, that member states have to ensure by appropriate means that audiovisual media services provided by media service providers under their jurisdiction do not contain any incitement to violence or hatred,[133] or public provocation to commit a terrorist offence.[134]

This includes an obligation on all providers to restrict access to content that is considered harmful for minors, meaning content that may impair the physical, mental or moral development of minors, without necessarily being illegal. Measures proposed by Article 6(a) of the AVMSD include selecting the time of the broadcast, age verification tools or other technical measures proportionate to the potential harm of the programme.

Since a significant share of the content provided on VSPs is not under the editorial responsibility of the VSP provider, Article 28(b) of the AVMSD specifies the obligation for member states to ensure that VSP providers under their jurisdiction shield users from harmful content and take appropriate measures to protect the general public from programmes, user-generated videos and audiovisual commercial communications containing such harmful content.[135] These measures must be necessary, effective and proportionate, balancing the need for user protection with the fundamental rights of platform providers and users, including the right to freedom of expression. Actions may include mechanisms for content reporting and flagging, age verification systems, parental control tools, and transparent content moderation procedures.[136]

While national regulatory authorities or bodies shall have the enforcement powers to ensure compliance under national law, member states shall encourage the use of co-regulation and the fostering of self-regulation through codes of conduct adopted at national level, which, *inter alia*, shall provide for effective enforcement including effective and proportionate sanctions.[137]

---

[133] As regards the scope see AVMSD, Article 6(1)(a).
[134] As set out in Article 5 of Directive (EU) 2017/541 of the Parliament and of the Council of 15 March 2017 on combatting terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88/6, 31 March 2017, which the AVMSD provision refers to.
[135] See Directive (EU) 2018/1808, op. cit, Recital 47.
[136] AVMSD, Article 28b(3).
[137] AVMSD, Article 4a(1). In addition, member states and the European Commission may foster self-regulation through Union codes of conduct, AVMSD, Article 4a(2).

Complementing the AVMSD, the European Media Freedom Act (EMFA)[138] introduced a new set of rules to protect media pluralism and independence in the EU. In addition, it includes rules on cooperation procedures between the national media regulatory authorities or bodies. With this, previous non-legally binding cooperation practices of the authorities and bodies under the umbrella of the European Regulators Group for Audiovisual Media Services (ERGA)[139] were formalised and thereby added to the AVMSD. Initially, the AVMSD had only established a cooperation body without specifying procedural details, although the need for close cooperation, in particular to resolve cross-border cases, had increased as a result of the extension of the scope of the AVMSD to VSPs.[140] Article 14 of the EMFA thus introduces a structured cooperation framework for the consistent and effective application of EMFA and the implementation of the AVMSD ensuring that there is dialogue and an obligation to justify actions on the part of the competent authority.[141] In addition, there is a specific provision concerning cooperation requests with regard to the obligations of VSPs (Article 15 of the EMFA) which reflects the pan-European nature of VSPs: while the providers operate their service regularly across borders in the EU, they are bound "only" to the jurisdiction of their country of origin member state, both under the ECD as well as under the AVMSD.[142]

The European Board for Media Services (EBMS) which replaces and succeeds the ERGA is, *inter alia*, tasked with ensuring coordinated enforcement across member states.[143] In addition, Article 17 of the EMFA contains a coordination rule within the EBMS concerning measures aimed at media service providers established outside the EU, which includes measures against "rogue media services" that present a serious and grave risk of prejudice to public security.[144] The latter is a direct reaction to difficulties observed when trying to achieve a common response to the risks created by the dissemination of Russian broadcast channels in the EU after the Russian Federation started the war against the Ukraine. The EBMS may coordinate national regulatory measures concerning media services targeting audiences in EU member states when such services, for example due to potential control by third-country governments or entities, pose a serious risk to public security or defence. In these cases, the EBMS can issue an opinion to promote a more unified and effective response.

---

[138] Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L 2024/1083, 17 April 2024.

[139] European Regulators Group for Audiovisual Media Services; see Memorandum of Understanding between the National Regulatory Authority Members of the European Regulators Group for Audiovisual Media Services (ERGA) of 3 December 2020 and Cole M.D. and Etteldorf C., "Future Regulation of Cross-Border Audiovisual Content Dissemination", Bd. 84 in *Schriftenreieh Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2023, pp. 149 *et seq.* and 176 *et seq*. The ERGA has been superseded by the EBMS, introduced by Article 8 of the EMFA.

[140] Recital 43 EMFA.

[141] See Cole M.D. and Etteldorf C., *Research for CULT Committee – European Media Freedom Act - Background Analysis*, European Parliament, Policy Department for Structural and Cohesion Policies, Brussels, 2023, p. 50.

[142] For a brief overview of the relationship between the AVMSD and the e-Commerce Directive see Oster J. and Wagner E., "*§ 38 Kommunikations- und Medienrecht*" in Ludwigs M. (ed.), *Handbuch des EU-Wirtschaftsrechts,* Beck C.H., 63rd amended ed. 2025, marginal No. 83 München, 2025.

[143] EMFA, Article 13.

[144] EMFA, Articles 13(l) and 17.

2.2.2.2. Regulating online platforms: the DSA and the DMA

Under the ECD, a regulatory system with a distinction between active and passive intermediaries evolved: liability was assigned depending on whether the intermediary remained neutral (passive) or whether his/her involvement went beyond passive hosting and (s)he interacted with the content, for example, by moderating, curating or optimising hosted content.[145] The liability exemptions based on this distinction that were previously contained in the ECD have now been incorporated into the Digital Services Act (DSA),[146] seeking to continue to reflect the varied roles of intermediaries with regard to third-party content although their roles have evolved significantly between the ECD and the DSA.[147]

The DSA seeks to reach "a safe, predictable and trusted online environment that facilitates innovation and in which fundamental rights enshrined in the EU Charter of Fundamental Rights,[148] including the principle of consumer protection, are effectively protected".[149] This includes a full harmonisation of the rules applicable to intermediary services in the internal market addressing the dissemination of illegal content online.[150] The concept of "illegal content" was meant to mirror in a broad way the existing rules for the offline environment.[151] Therefore, the DSA's definition of "illegal content" is broad, referring to "any information that, in itself or in relation to an activity, including the sale of products or the provision of services, is not in compliance with Union law or the law of any member state which is in compliance with Union law, irrespective of the precise subject matter or nature of that law".[152] This should cover content that under the applicable law is either itself illegal, such as illegal hate speech or terrorist content and unlawful discriminatory content, or that the applicable rules render illegal in view of the fact that it relates to illegal activities.[153]

Recital 12 of the DSA provides illustrative examples of illegal content including the sharing of images depicting child sexual abuse, the unlawful non-consensual sharing of private images, online stalking, the sale of non-compliant or counterfeit products, the sale of products or the provision of services in infringement of consumer protection law, the non-authorised use of copyright protected material, the illegal offer of accommodation

---

[145] See Cole M.D., Etteldorf C. and Ullrich C., *Cross-Border Dissemination of Online Content*, Bd. 81 *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2020, pp. 176 *et seq*.; Rowland D., Kohl U. and Charlesworth A., *Information Technology Law*, Routledge, Abingdon, 5th ed. 2017, pp. 104 *et seq*.; Schmitz S., *The Struggle in Online Copyright Enforcement*, Nomos, Baden-Baden 2015, pp. 574 *et seq*.

[146] European Union, 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 277/1, 27 October 2022.

[147] Cole M.D., Etteldorf C. and Ullrich C., *Cross-Border Dissemination of Online Content*, Bd. 81 *Schriftenreihe Medienforschung der LfM NRW*, Nomos, Baden-Baden, 2021, pp. 222 *et seq*; Buiten, M.C., "The Digital Services Act – From Intermediary Liability to Platform Regulation", in *JIPITEC*, 12, 2021, pp. 361-380; Madiaga T., *Reform of the EU liability Regime for Online Intermediaries, Background on the forthcoming Digital Services Act,* European Parliamentary Research Service, PE 649.404, Brussels, May 2020.

[148] *Charter of Fundamental Rights of the European Union*, 2012/C 326/02, OJ C 326/391, 26.10.2012.

[149] DSA, *op. cit*., Article 1(1).

[150] Ibid., Recital 9.

[151] Ibid, Recital 12.

[152] Ibid, Article 3(h).

[153] Ibid., Recital 12.

services or the illegal sale of live animals. For this purpose, the DSA establishes, through harmonised rules for the provision of intermediary services, in particular a framework for the conditional exemption from liability for providers of intermediary services (Article 1(2)(a) of the DSA), and – separate from questions of liability – specific due diligence obligations tailored to certain categories of intermediary service providers (Article 1(2)(b) of the DSA).

Chapter II of the DSA sets out the liability rules for intermediary service providers: mere conduit (Article 4 of the DSA), caching (Article of the 5 DSA) and hosting (Article 6 of the DSA).[154] Mere conduits and caching services are not liable for transmitted or stored information if they do not interfere with it. Host providers are exempted from liability for content stored on behalf of users unless they have actual knowledge of the illegal activity or content and fail to act expeditiously to remove or to disable access to that content.[155] Actual knowledge or awareness can arise through various channels, including own-initiative investigations or through third-party notices, provided these are sufficiently precise and adequately substantiated to allow a diligent economic operator to identify, assess, and where appropriate, act against the allegedly illegal content.[156] Hosting providers, regardless of their size, must implement easily accessible and user-friendly notice and action mechanisms to facilitate such notifications. There is no set time frame for the removal of content other than the "expeditious" action required by Article 6(1)(b) of the DSA. In order to achieve faster action against illegal content, the DSA foresees that notices submitted by so-called "trusted flaggers"[157] operating within the regulatory framework of the DSA have to be prioritised in the treatment by the intermediaries.[158] The status of a trusted flagger is awarded by the Digital Service Coordinator (DSC) of the member state in which the applicant for such a role is established and only to a limited number of entities that have demonstrated particular expertise and competence in identifying illegal content.[159] Said expertise may also be limited to a specific subject area, the "designated area of expertise",[160] such as the expertise of HateAid gGmbH in Germany in the field of cyber violence and illegal speech. With regard to transparency, the trusted flaggers are under an obligation to publish easily comprehensible and detailed reports on notices submitted and, *inter alia*, the action taken by the respective provider in response.[161] The European Commission is currently preparing guidelines on trusted flaggers that aim to

[154] For an overview of the liability regimes under the DSA see Capello M. (ed.), "*Unravelling the Digital Services Act Package*", *IRIS Special*, European Audiovisual Observatory, Strasbourg, 2021, pp. 13 *et seq*.
[155] Article 6 DSA.
[156] See Recital 22 and Article 6 DSA. On the requirement of "actual knowledge" see Radtke T., "Article 6 DSA" in Gersdorf H. and Paal B. (eds.), BeckOK Informations- und Medienrecht, Beck C. H., München, 48th ed., 2025, paragraphs 27 *et seq*.
[157] On trusted flaggers see van de Kerkhof J., "Article 22 Digital Services Act: Building Trust with Trusted Flaggers", *Internet Policy Review*, 14(1), 2025. For an overview see also https://digital-strategy.ec.europa.eu/en/policies/trusted-flaggers-under-dsa.
[158] DSA, *op. cit.*, Article 22(1).
[159] Ibid., Article 22(2). As of 25 August 2025, 38 trusted flaggers have been designated.
[160] Ibid., Article 22(1).
[161] Ibid., Article 22(3).

assist DSCs by streamlining the process of appointing trusted flaggers and also providing guidance on circumstances that can lead to revoking the status.[162]

While the obligations concerning removal of illegal content on notification in order to avoid liability concern all intermediaries, some additional due diligence obligations are applicable for those very large online platforms (VLOPs) or very large online search engines (VLOSEs) that, due to their significant reach, have a societal impact that brings risks with it. The operational threshold is set at 45 million monthly users, a number equivalent to 10% of the EU population.[163] The obligation to carry out risk assessments as well as risk mitigation measures extends to the dissemination of illegal content and anticipated negative effects on human rights. The risks associated with the spread of illegal content as well as certain harmful content must be diligently noticed, analysed and addressed.[164] Measures have to be reasonable and effective, while at the same time proportionate to the economic capacity of the provider.[165] As such they can include the possible adoption of specific provisions in the terms and conditions, potential adaptations of content moderation systems and internal processes of decision-making.[166] This does not mean that there is a mandatory monitoring obligation, since Article 8 of the DSA stipulates that there is no general monitoring or active fact-finding obligation. Rather, the DSA mentions content moderation as a factor having an impact on the level of risk of dissemination of illegal content.[167]

Pursuant to Article 3(f) of the DSA, "content moderation" means the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions which has been shared by recipients of the service. Such measures include influencing the availability, visibility, and accessibility of that illegal content, such as by demotion, demonetisation, disabling of access to, or removal thereof. Another way to react is to affect the ability of the recipients of the service to provide information, such as the termination or suspension of a recipient's account. The details of how moderation processes and systems are designed — including individual decisions and large-scale moderation — are left to the discretion of the implementing company. At the same time, however, the DSA imposes clear obligations to remove certain types of content promptly.

Adherence to and compliance with codes of conduct under Article 45 of the DSA may serve as a valid risk mitigation measure. In particular, risk mitigation measures concerning specific kinds of illegal content should be explored via self- and co-regulatory measures including codes of conduct.[168] The existing codes of conduct relating to significant systemic risks predate the DSA as self-regulatory measures in the form of codes of practice. Drawing on these pre-existing codes of practice, these codes can become codes of conduct under the DSA. Article 45 of the DSA sets out a number of criteria for that, including the

[162] The adoption is planned before the end of 2025.
[163] DSA, op. cit., Article 33. As of 25 August 2025, 33 VLOPs and two VLOSEs have been designated.
[164] Ibid., Recitals 53 and 55.
[165] Ibid., see Recital 86.
[166] Ibid., Recital 87.
[167] Ibid., Articles 34(2)(b) and 35(1)(c).
[168] Ibid., see Recital 104.

need to have specific objectives, key performance indicators and take due account of the needs and interests of all interested parties. The European Commission and the newly established European Board for Digital Services (EBDS)[169] are tasked with assessing whether a code meets the aim of contributing to the proper application of the DSA.[170]

Besides imposing obligations on intermediary services, the DSA establishes a comprehensive framework to ensure compliance with these obligations. The enforcement of the DSA involves a range of investigative and sanctioning measures available to both national authorities and the European Commission depending on the allocation of supervisory competences depending on the different types of providers.

To this end, member states are obliged to designate one or more independent competent authorities responsible for the supervision of providers and the enforcement of the DSA. The DSA, however, does not require member states to confer on competent authorities the task of adjudicating on the lawfulness of specific items of content. Civil, criminal and administrative law responses including, for instance, requests to remove illegal content are governed by the national laws of the member states.[171] Member states must lay down rules on effective, proportionate and dissuasive penalties which can be applied in the event of DSA infringements falling within their competence.[172] Given the cross-border nature of the services concerned and the horizontal range of obligations, each member state must in addition identify a DSC to act as the single contact point in the context of supervision and enforcement at Union level.[173] The EBDS serves as an independent advisory group to ensure uniform application of the DSA and support effective cooperation between the European Commission and the DSCs.[174]

For enforcement vis-à-vis providers of VLOPs and VLOSEs (jointly called VLOPSEs), the DSA assigns the competence to the European Commission, which thus becomes a regulatory authority. Pursuant to Articles 65 *et seq*. of the DSA, the European Commission may exercise investigatory powers on its own initiative and initiate proceedings against this category of providers. Besides investigatory powers, the European Commission can adopt a decision on non-compliance and impose fines or periodic penalty payments.[175] A breach of the DSA is punishable with a fine of up to 6% of the global turnover of the VLOPSEs concerned and may also trigger an enhanced supervision period to ensure compliance.[176] If the situation is urgent, interim measures can be imposed; in the event of persistent infringement with serious harm to users and entailing criminal offences involving a threat to a person's life and safety even the temporary suspension of the service can be requested.[177]

---

[169] DSA, op. cit., see Article 61.
[170] Ibid., Article 45(4).
[171] See, for instance Zurth P., "Private Rechtsdurchsetzung im Digital Services Act", *Gewerblicher Rechtsschutz und Urheberrecht*, 125(19), 2023, pp. 1329-1408, 1331.
[172] Ibid., Article 52.
[173] Ibid., Article 49(2) and recital 110.
[174] Ibid., Article 61.
[175] Ibid., Articles 73-74, 76 and 79.
[176] Ibid., Articles 74-75.
[177] Ibid., Articles 82 and 51(3).

The investigation and enforcement powers of the European Commission are complemented by transparency mechanisms in order to ensure an adequate level of transparency and accountability. All intermediary services are obliged to publish an annual transparency report on any content moderation that they engaged in during the period.[178] This includes, *inter alia*, information on the number of orders received from member state authorities, their content moderation practices, the number of items removed, as well as the number of notices submitted by trusted flaggers or other removal requests. In view of their systemic risks, providers of VLOPSEs have increased reporting obligations that extend to human resources and their qualifications as well as the publication of reports every six months.[179] In addition, the European Commission launched a transparency database pursuant to Article 24(5) of the DSA, which collects and makes publicly available the mandatory statement of reasons[180] that VLOPSEs have to provide whenever they remove or otherwise restrict access to content.

While the European Commission has not yet issued any fines under the DSA – although several proceedings are ongoing, namely concerning obligations regarding the protection of minors[181] – concerning the Digital Markets Act (DMA)[182] the European Commission has already taken enforcement actions.[183] The objective of the DMA is to create a "contestable and fair market"[184] in the digital sector and it primarily addresses competition issues in relation to "core platform services" (CPS) offered by so-called "gatekeepers". Article 2(2) of the DMA provides the list of services that are considered to be CPS including online search engines, online social networking services, video-sharing platform services and online advertising services, while Chapter II of the DMA details the designation of the providers as gatekeepers. Similar to the concept of VLOPSEs under the DSA, gatekeepers have a significant impact on the internal market and provide one (or more) of the selected CPS which serve as an important gateway for business users to reach end users. The position of the undertaking must be "entrenched and durable" either currently or foreseeably in the near future.[185] Accordingly, gatekeepers are undertakings with systemic relevance. The numerical thresholds for this as set out in Article 3(2) of the DMA are very high, but so far 23 CPS have already been designated and are provided by seven distinct gatekeepers.[186]

---

[178] Article 15 of the DSA. See also Etteldorf C., "A Major Milestone in the EU: The Digital Services Act Package" in Capello M. (ed.), *Algorithmic Transparency and Accountability of Digital Services, IRIS Special*, European Audiovisual Observatory, Strasbourg, 2023, pp. 31 and 39.

[179] DSA, op. cit., Article 42.

[180] Article 17 of the DSA.

[181] See e.g. European Commission, Commission Decision Initiating Proceedings pursuant to Article 66(1) of Regulation (EU) 2022/2065 of 18 December 2023 against Twitter International Unlimited. For an overview of the main enforcement activities see the dedicated Commission website.

[182] European Union, 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), OJ L 265/1, 12 October 2022.

[183] On 23 April 2025, the Commission fined Apple €500 million and Meta €200 million, see European Commission, "Commission finds Apple and Meta in breach of the Digital Markets Act", Press release, 23 April 2025.

[184] On the latter see Cole M.D., "The Proposal for a Digital Markets Act (DMA): On Gatekeepers, Fairness and Transparency in the Online Environment" in Capello M. (ed.), *Unravelling the Digital Services Act Package*, *IRIS Special*, European Audiovisual Observatory, Strasbourg, 2022.

[185] DMA, op. cit., Article 3.

[186] A dedicated Commission website lists the designated gatekeepers.

The DMA defines for the online sector types of behaviour that are to be regarded as abusive if applied by gatekeepers and introduces a number of specific obligations and prohibitions for gatekeepers. These include rules on advertising information including access to information about the functioning of online advertising value chains (Articles 5(9), (10) and 6(8) of the DMA), and on the ranking of content (Article 6(5) of the DMA).

As regards enforcement, the DMA differs from the DSA's multi-actor approach by centralising the enforcement at the European Commission. It has the power to open market investigations,[187] open proceedings with the possible adoption of decisions pursuant to compliance with the obligations for gatekeepers and the imposition of fines on gatekeepers including fines of up to 20% of their worldwide annual turnover for repeated infringements.[188]

2.2.2.3. Regulating online political advertising: the TTPAR

In view of its capacity to reach audiences the Internet, unsurprisingly, is used extensively by political parties and politicians to impart their political opinions or "to convey a political message".[189] In that context, in particular, microtargeting based on profiling using machine learning and AI present a significant threat, not only to personal autonomy but also to democracy itself. The latter was exposed, *inter alia*, by the Cambridge Analytica scandal.[190] As a regulatory response, the Transparency and Targeting of Political Advertising Regulation (TTPAR)[191] of April 2024 seeks to address the concerns related to information manipulation and foreign interference in elections by harmonising the rules on the transparency and related due diligence obligations for the provision of political advertising services. The TTPAR complements, *inter alia*, the DSA, DMA and the General Data Protection Regulation (GDPR) with a view to safeguarding electoral integrity considering the difficult regulatory and enforcement challenges in the digital age.

The TTPAR introduces a wide definition of political advertising defined as a message (a) by, for, or on behalf of a "political actor", unless it is of a purely private or a purely commercial nature; or (b) which is liable to influence the outcome of an election or referendum, a legislative or regulatory process, or voting behaviour. The notion of political actors is also defined in Article 2 to include a wide range of actors, including political parties, candidates and political campaign organisations. Chapter II of the TTPAR sets out rules on transparency for political advertising including transparency notices and sponsor information, meaning, *inter alia*, that each political advertisement has to be labelled as such and provide information about the sponsor and any potential entity controlling the sponsor.[192] Thereby, the TTPAR introduces prohibitions on certain types of content disseminated online, namely if it is "unlabelled" political advertising. The TTPAR moreover

[187] DSA, op. cit., Articles 16-19.
[188] Ibid., Articles 20, 29-30.
[189] See *Magyar Kétfarkú Kutya Párt v. Hungary*, No. 201/17 (ECtHR, 20 January 2020), paragraphs 88-89.
[190] See Dowling M.-E., "Cyber Information Operations: Cambridge Analytica's Challenge to Democratic Legitimacy", *Journal of Cyber Policy*, 7(2), 2022, pp. 230-248.
[191] European Union, Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising (TTPAR), OJ L 2024/900, 20 March 2024.
[192] Ibid., Article 11(1).

imposes a ban on political advertising coming from sponsors from outside the EU in the three months leading up to an election or referendum.[193] Under the transparency obligations of Article 12 of the TTPAR, when political advertising involves the use of targeting or amplification techniques based on personal data, data controllers are required to accompany the advertisement with additional information enabling the individual to understand the logic behind the technique, the key parameters guiding its use, and whether third-party data or additional analytical methods were applied. With a view to further transparency, Article 13 of the TTPAR requires the European Commission to establish a European repository for online political advertisements similar to the advertising repositories that certain intermediaries have to provide under the DSA.

The supervision and enforcement involves various actors including data protection authorities and imposes an obligation on member states to designate one or more competent authorities for the effective application, supervision and enforcement of the TTPAR.[194] These authorities are entrusted with various investigative and enforcement tools including data access requests, the competence to issue warnings or impose fines.[195] In view of the cross-border nature of certain online political advertisements, the TTPAR also establishes rules concerning jurisdiction: where a service provider offers the services in more than one member state, the competent authority or authorities of the member state where the main establishment of the provider of political advertising services is located should usually be responsible.

In carrying out their supervisory and enforcement powers, the competent authorities of all member states should, however, cooperate with and assist each other as necessary and to this end make use of existing structures, including national cooperation networks, the European Cooperation Network on Elections,[196] the EBDS and EBMS (formerly the ERGA).[197] In that regard, rules on cross-border cooperation are provided in Article 23 of the TTPAR including a cross-border notification procedure. Sanctions include fines of up to 6% of the annual income or budget of the sponsor or of the provider of political advertising services, whichever is the highest, or 6% of the annual worldwide turnover of the sponsor or the provider of political advertising services in the preceding financial year. Member states may also lay down rules on other measures including periodic penalty payments.[198]

[193] TTPAR, op. cit., Article 5(2). "Election" or "referendum" refers to any such type of electoral process organised at Union level or at national, regional or local level in a member state.
[194] Ibid., Article 22(1)-(4), which stipulates that for different supervision and enforcement tasks the competent authorities may differ.
[195] Ibid., Article 22(5).
[196] See European Commission, Terms of Reference, European Cooperation Network on Elections.
[197] TTPAR, Article 22(8).
[198] TTPAR, Article 25 and Recital 104.

2.2.2.4. Regulating content relating to personal data: the GDPR

The GDPR[199] as the primary legal framework governing the processing of personal data sets forth principles of and rules on the protection of natural persons with regard to said processing in view of rapid technological developments and globalisation.[200] Article 3 of the GDPR extends the territorial scope of the regulation to include, *inter alia*, the activities of EU controllers and processors regardless of whether the processing takes place in the EU or not, and to data controllers and processors established outside the EU if they offer goods or services to a data subject in the EU. For these data controllers and processors the GDPR establishes obligations ranging from data minimisation as a principle to notification obligations in the event of data breaches. Data subjects are granted numerous rights with regard to the processing of their personal data, such as the right to obtain information about whether their personal data is being processed (Article 15), a right to the rectification of inaccurate or incomplete data (Article 16), a right to erasure (Article 17) or a right to object to the processing of personal data (Article 21).

The enforcement regime of the GDPR combines national enforcement mechanisms, cross-border cooperation and coordination rules. As part of the administrative enforcement scheme, independent national supervisory authorities should be established by each member state,[201] and these are to observe the cooperation mechanisms foreseen in the GDPR. [202]

They are vested with extensive investigatory and enforcement powers.[203] Each Data Protection Authority (DPA) has jurisdiction to investigate GDPR complaints within the territory of its own member state, and in order to achieve a consistent application of the GDPR, to cooperate with other DPAs under the so-called "consistency mechanism" involving the European Data Protection Board (EDPB).[204] Under the GDPR's one-stop-shop mechanism, a lead supervisory authority, which is the DPA of the controller's main establishment in the EU, has jurisdiction when a case is of a cross-border nature, but other concerned DPAs have to be provided with information and may oppose a proposed decision by the lead authority.[205] Issues and challenges encountered in this enforcement system involving various actors are addressed in a new procedural regulation aimed at harmonising the

[199] European Union, 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 [2016] OJ L 119/1.
[200] See Recitals 1 *et seq*. of the GDPR.
[201] Articles 51 *et seq*. of the GDPR.
[202] For how the GDPR regime seeks to respond to the challenges encountered under the Data Protection Directive, see Giurgiu A. and Larsen T.A., "Roles and Powers of National Data Protection Authorities: Moving from Directive 95/46/EC to the GDPR: Stronger and More 'European' DPAs as Guardians of Consistency?", in *European Data Protection Law Review*, 2(3), 2016, pp. 342 – 352.
[203] Article 58 of the GDPR.
[204] Article 63 of the GDPR.
[205] For an outline of the Article 60 GDPR cooperation mechanisms see Hijmans H., "The DPAs and their Cooperation: How Far Are We in Making Enforcement of Data Protection Law more European?", in *European Data Protection Law Review*, 2(3), 2016, pp. 362 – 372.

requirements for the admissibility and procedures of cross-border action.[206] Article 83 of the GDPR empowers supervisory authorities to impose significant administrative fines of up to EUR 20 million or up to 4% of global annual turnover, whichever is higher. Member states shall also lay down rules on other penalties for non-compliance.[207]

Although the GDPR is not designed specifically to target illegal content or disinformation, it indirectly plays an important role in how such content can be addressed by regulating the use of personal data in content moderation, profiling, and content targeting. For instance, by imposing restrictions on how personal data can be used for microtargeting, the GDPR addresses a key vector in the spread of disinformation. The principles of data minimisation and purpose limitation put further constraints on targeting systems. In addition, Article 17 of the GDPR with the "right to be forgotten" requires DPAs to ensure, at the request of the data subject, that intermediaries take down content where the retention of such data infringes the GDPR, EU or member state law to which the controller is subject. In particular, a data subject has the right to have his or her personal data erased where the data is no longer necessary or relevant.[208]

2.2.2.5. Regulating communication technology: the AI Act

The AI Act[209] is a product safety regulation introducing rules on the safety of the regulated technology, but unlike traditional safety laws, the AI Act also protects fundamental rights, regulates the uses of AI and involves ethical principles. It is therefore not directly concerned with the enforcement of content-related rules as was the case with the GDPR, but it can nevertheless play a supportive role in addressing the risks of disinformation and illegal content, particularly when content is generated or amplified by AI systems. This is especially the case because the AI Act explicitly addresses the phenomenon of so-called deepfakes, that is, AI-generated or manipulated images, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful.[210] Accordingly, it complements other digital laws by adding a further layer of obligations for the use of AI systems.

Similarly to the DSA, the AI Act, as a risk-based regulation, introduces obligations regarding transparency, accountability and risk mitigation. Different obligations are introduced depending on the level of risk of an AI system. AI practices which bear an

[206] Regulation (EU) 2025/2518 of the European Parliament and of the Council of 26 November 2025 laying down additional procedural rules on the enforcement of Regulation (EU) 2016/679 [2025] OJ L 2025/2518. For an overview and assessment of the Commission Proposal see Mustert L., "The Commission Proposal for a New GDPR Procedural Regulation: Effective and Protected Enforcement Ensured?", *European Data Protection Law Review*, 9(4), 2023, pp. 454 – 464.
[207] Article 84 GDPR.
[208] C-131/12 *Google Spain SL, Google Inc. v. AEPD* [2014] ECLI:EU:C:2014:317*;* see also Pouillaude S., "Harmonising the Enforcement of the Right to Be Forgotten: Navigating New Speech Regulation Challenges in the EU", *European Data Protection Law Review*, 10(2), 2024, pp. 162 – 177.
[209] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No. 300/2008, (EU) No. 167/2013, (EU) Nos. 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 [2024] OJ L 2024/1689.
[210] Article 3(60) of the AI Act.

unacceptable risk are prohibited under Article 5 of the AI Act; this includes an AI system that deploys purposefully manipulative or deceptive techniques causing a person to make a decision that he or she would otherwise not have made. In contrast, high-risk AI systems under Article 6 of the AI Act are AI systems that pose a significant risk to the health, safety, or fundamental rights of individuals, and are subject to strict legal obligations and oversight. Requirements that apply to these systems include, *inter alia*, risk management, technical documentation and record-keeping, transparency and human oversight.[211] The AI Act imposes specific rules for general-purpose AI systems that pose systemic risks such as actual or reasonably foreseeable negative effects on democratic processes and the dissemination of illegal, false, or discriminatory content.[212] In addition, transparency obligations are imposed on providers and deployers of AI systems with limited risks, namely systems that, for instance, are intended to interact directly with natural persons (such as chatbots), or generate manipulated audio, image, video or text content.[213] As an example, AI systems used to generate or manipulate image, audio or video content that appreciably resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful, so-called deepfakes, must be cleary labelled as artificially created or manipulated and must disclose the artificial origin.[214] This ensures that users are aware that they are viewing synthetic content. Content that is not labelled in accordance with Article 50 of the AI Act is unlawful.

Enforcement and supervision of the AI Act follows the New Legislative Framework of the EU for product legislation,[215] which created a toolbox of measures for use in product legislation. Member states have to establish or designate at least one notifying authority and at least one market surveillance authority who exercise their powers independently and impartially.[216] Market surveillance authorities supervise and enforce compliance with the rules for AI systems, including prohibitions and rules for high-risk AI, whereas notifying authorities designate and supervise notified bodies, which are independent bodies that conduct pre-market conformity assessments. In that context, it must be noted that for high-risk AI systems, enforcement is embedded in an *ex-ante* conformity assessment system. A new AI office[217] at the EU level ensures harmonised enforcement and oversight, in particular in relation to general-purpose AI models.[218] The AI office is thus vested with investigatory and enforcement powers.[219] In addition, Article 65 of the AI Act establishes a European Artificial Intelligence Board, which is, *inter alia*, tasked with contributing to the coordination among national competent authorities and contributing to the harmonisation of administrative practices in the member states.[220] The AI Act includes graduated administrative fines, which range from up to EUR 35 million or 7% of the global annual turnover, whichever is higher, for non-compliance with the prohibited AI practices in Article

[211] Articles 8 *et seq*. of the AI Act.
[212] See Article 55 and Recital 110 of the AI Act.
[213] Article 50 of the AI Act.
[214] Article 50(4) of the AI Act.
[215] See the dedicated website of the European Commission.
[216] Article 70 of the AI Act.
[217] Article 64 of the AI Act.
[218] See Article 88 of the AI Act.
[219] See Articles 88 *et seq*. of the AI Act.
[220] Article 66 of the AI Act.

5 of the AI Act to up to EUR 7.5 million or 1% of the global annual turnover, whichever is higher, for incorrect, incomplete or misleading information to notified bodies or national competent authorities in reply to a request for information.[221]

2.2.2.6. Further approaches to regulating content deemed illegal

Besides the EU secondary legislation outlined above, sector-specific instruments also regulate online content deemed illegal and increasingly harmonised criminal law provisions emerge.

As regards content related to terrorism, the Terrorist Content Regulation (TERREG)[222] foresees enforcement mechanisms and requires platforms to take selective action against prohibited content. The TERREG mandates hosting service providers, which offer services in the EU, to take down terrorist content within one hour after receipt of a removal order.[223] Accordingly, the TERREG establishes a rapid response model with direct enforcement by the national competent authorities under the TERREG; these authorities are tasked with issuing removal orders as well as imposing penalties. Member states must lay down rules on administrative penalties applicable to infringements of the TERREG and ensure that systematic or persistent failure to comply with removal orders is subject to financial penalties of up to 4% of the provider's global annual turnover.[224] The TERREG also prescribes cooperation between national competent authorities, host service providers and Europol.[225] The application of the TERREG is overseen by the European Commission, to which member states have to report annually on actions taken in accordance with the TERREG including the number of removal orders.

Further EU legislative instruments seek to harmonise the illegality of certain behaviours online such as the Directive on combatting violence against women and domestic violence[226] which renders cyber incitement to violence or hatred on the ground of gender a criminal offence as well as the non-consensual sharing of intimate images, but provides no specific enforcement mechanism other than the encouragement of self-regulatory cooperation between relevant intermediaries such as the establishment of codes of conduct. The criminalisation of hate speech is further addressed with the Council Framework Decision 2008/913/JHA[227] which provides a baseline for the criminalisation of hate speech and hate crimes across member states, covering racist and xenophobic content. Although as an instrument of intergovernmental cooperation not directly applicable, Council Framework Decision 2008/913/JHA requires member states to transpose its provisions into national law and thereby approximates the laws of member states. In

[221] Article 99 of the AI Act.
[222] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172/79, 17 May 2021.
[223] Article 3 of the TERREG.
[224] Article 18 of the TERREG.
[225] Article 14 of the TERREG.
[226] European Union, Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combatting violence against women and domestic violence, OJ L 2024/1385, 24 May 2024.
[227] Council Framework Decision 2008/913/JHA of 28 November 2008 on combatting certain forms and expressions of racism and xenophobia by means of criminal law, OJ L 328/55, 6 December 2008.

addition, the proposal for a regulation laying down rules to prevent and combat child sexual abuse[228] seeks to introduce obligations for risk assessment and mitigation, the detection, reporting and removal of child sexual abuse material, potentially extending to proactive scanning measures by online platforms, which is controversially discussed.[229] The proposal seeks to address the weaknesses of a prior directive,[230] that required the removal and blocking of said material but did not lay down more detailed rules on the procedure. A second mechanism in the directive provided a framework for member states to take measures to block foreign websites that share child sexual abuse material. However, since the implementation was voluntary, only half of the member states introduced specific national legislation.

2.2.3. Measures targeting illegal and harmful content under the CFSP

Under the EU's Common Foreign and Security Policy (CFSP), the EU has adopted targeted measures to address the dissemination of illegal and harmful content by foreign actors, particularly in the context of disinformation campaigns and cyber threats. These measures are typically enacted through Council decisions and regulations imposing restrictive measures against individuals or entities responsible for conducting or supporting foreign information manipulation and interference (FIMI) operations that threaten the security, democracy, or public order of the EU or its member states. In response to Russia's war against Ukraine, the EU took action leading to the suspension of the broadcasting activities and licences of several Russian state-controlled media outlets.[231] Since revocation of licences did in practice not prevent the dissemination of content in the EU, the Council of the EU imposed sanctions in the form of a decision and a regulation which prohibited operators from broadcasting or otherwise contributing to the broadcasting of the content of certain state-controlled media outlets (namely RT and Sputnik) within the EU, citing their role in spreading distortion of facts and disinformation.[232] These measures were

[228] European Commission, Proposal for a Regulation of the European Parliament and of the Council Laying Down Rules to Prevent and Combat Child Sexual Abuse COM(2022) 209 final, 2022.
[229] Leiser, M.R. and Murray, A.D., "Rethinking Safety-by-Design and Techno-Solutionism for the Regulation of Child Sexual Abuse Material", in *Technology and Regulation*, 2025, pp. 131 – 171.
[230] Directive 2011/93 of the European Parliament and of the Council of 13 December 2011 on combatting the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA OJ L 335/1, 17 December 2012.
[231] See overview by Cabrera Blázquez F.J., "European Commission: Banning of Russia Today and Sputnik", IRIS 2022-3:1/6, European Audiovisual Observatory, Strasbourg, 2022 and *The Implemenation of EU Sanctions against RT and Sputnik*, European Audiovisual Observatory, Strasbourg, 2022; Cole M.D. and Etteldorf C., *Future Regulation of Cross-Border Audiovisual Content Dissemination*, Bd. 84 Schriftenreieh Medienforschung der LfM NRW, Nomos, Baden-Baden, 2023, pp. 217 *et seq*.
[232] European Union, Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 65/1, 2 March 2022; and Council Decision (CFSP) 2022/351 of 1 March 2022 amending Decision (EU) 2014/512/CFSP concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 65/1, 2 March 2022.

subsequently extended to several other Russian media outlets[233] and confirmed as fundamental rights compatible by the General Court of the EU. An application by a Dutch coalition of Internet service providers and media organisations to the CJEU seeking the annulment of the orders concerning the prohibitions of disseminating or supporting the dissemination of the sanctioned entities' content was unsuccessful.[234] Further restrictive measures upon Russian entities followed, that also targeted individuals for conducting a disinformation campaign.[235]

These actions, grounded in the EU's external action competence, demonstrate the CFSP's evolving role in countering foreign information threats and complementing internal regulatory efforts under instruments like the DSA. Moreover, they help to understand the the evolving regulatory framework, for instance the rules on rogue media services and the accelerated cooperation under the EMFA.[236]

Under what was the second pillar of the EU on common foreign and security policy, the European External Action Service (EEAS) has also been particularly active in tackling disinformation. Since 2015, the EEAS has been reporting regularly on disinformation including attempts at election interference and FIMI activities on its awareness raising project website "EUvsDisinfo"[237] and social media based on the Conclusions of the European Council on External Relations of 19 March 2015[238] and subsequently under the Action Plan

[233] E.g. Council Regulation (EU) 2022/879 of 3 June 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 153/53, 3 June 2022 and Council Implementing Regulation (EU) 2022/994 of 24 June 2022 implementing Regulation (EU) 2022/879 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ LI 167/1, 24 June 2022; Council Regulation (EU) 2022/2474 of 16 December 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ LI 322/1, 16 December 2022 and Council Implementing Regulation (EU) 2023/180 of 27 January 2023 implementing Regulation (EU) 2022/2474 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 26/1, 30 January 2023; Council Regulation (EU) 2023/427 of 25 February 2023 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ LI 59/6, 25 February 2023 and Council Implementing Regulation (EU) 2023/722 of 31 March 2023 implementing Regulation (EU) 2023/427 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine, OJ L 94/19, 3 April 2023.

[234] T-307/22 *A2B Connect and Others v Council* (GC, 26 March 2025) ECLI:EU:T:2025:331. See also previously T-125/22 RT France v Council (GC, 27 July 2022) ECLI:EU:T:2022:483.

[235] Council Decision (CFSP) 2023/1566 of 28 July 2023 amending Decision 2014/145/CFSP concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, OJ LI 190/21, 28 July 2023; Council Implementing Regulation (EU) 2023/1563 of 28 July 2023 implementing Regulation (EU) No 269/2014 concerning restrictive measures in respect of actions undermining or threatening the territorial integrity, sovereignty and independence of Ukraine, OJ LI 190/1, 28 July 2023.

[236] See in that regard Eskens S., "The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy", *in* Computer Law & Security Review, 58, 2025, 106185.

[237] See https://euvsdisinfo.eu/.

[238] European Council, European Council meeting (19 and 20 March 2015) – Conclusions, (2015) EUCO 11/15.

against Disinformation of the High Representative for Foreign Affairs and Security Policy of 5 December 2018[239].

In 2022, the EEAS adopted a Strategic Compass on Security and Defence, which foresaw the development of a FIMI Toolbox to strengthen the ability to detect, analyse and respond to the threat and further enhance the EU's strategic communication and counter disinformation capabilities.[240] The toolbox addresses different areas and outlines short-, medium- and long-term measures to tackle FIMI. The measures range from pre-incident countermeasures, such as media literacy programmes, through minimising countermeasures, such as removing online content depending on existing regulations or mechanisms, to post-incident countermeasures including information sharing and the deployment of legal responses and sanctions.[241] Similar to the field of cybersecurity, a great emphasis is put on information sharing to increase the level of preparedness. Accordingly, in 2023, the FIMI Information Sharing and Analysis Centre (FIMI-ISAC) was established as a community-based network with civil society and other stakeholders.[242]

[239] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, Action Plan against Disinformation, JOIN(2018) 36 final.
[240] EEAS, *A Strategic Compass for Security and Defence*, 2022, p. 40.
[241] EEAS, *2nd EEAS Report on Foreign Information Manipulation and Interference Threats*, January 2024, pp. 17 *et seq*.
[242] EEAS, *EEAS Stratcom's Responses to Foreign Information Manipulation and Interference (FIMI) in 2023*, Press release 28 June 2024.

3. Countering disinformation

3.1. Enforcement at EU level

Dr Mark D. Cole, Director for Academic Affairs, Institute of Europea Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

Disinformation can take many forms and there are many types that are commonly seen as problematic. It can encompass political disinformation,[243] health disinformation,[244] conspiracy theories,[245] deepfakes[246] and manipulated media[247] as well as foreign influence operations. Furthermore, scams such as fake investment schemes, or social and cultural manipulation such as false stories seeking to stir racial, religious, or ethnic tensions may fall under the umbrella term, when false or misleading content is used to trick people for economic gain or to cause public harm.

The following section focuses on state-driven disinformation as an example of how the scale and quality of disinformation campaigns have intensified in the EU. In parallel, a strengthening of measures and enforcement by means of hard law solutions can be observed.

At the EU level, various initiatives against disinformation have been taken since 2015 when the European Council emphasised "the need to challenge Russia's ongoing disinformation campaigns"[248] after the illegal annexation of Crimea by Russia in 2014. While the first policy measures focused on so-called "hybrid threats" (i.e. harmful activities by state and non-state actors using a mixture of military and non-military methods without formally declaring warfare),[249] subsequent measures aimed to broaden the scope of these initiatives to "disinformation", understood as "verifiably false or misleading information that is

[243] See European Commission, "Digital Services Act – Application of the Risk Management Framework to Russian Disinformation Campaigns", Publications Office of the European Union, Luxembourg, 2023.
[244] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Tackling COVID-19 Disinformation – Getting the facts right, Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions, 2020.
[245] See the dedicated website "Identifying Conspiracy Theories" by the European Commission.
[246] Europol, "Facing Reality? Law Enforcement and the Challenges of Deepfakes", Publications Office of the European Union, Luxembourg, 2022, pp. 10 *et seq*.
[247] Marwick, A. and Lewis, R. *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017; Wardle, C. and Derakhshan, H., "Information Disorder: Toward an Interdisciplinary Framework for Research and Policy Making", Council of Europe Report DGI(2017)09, pp. 20 et seq. See also the dedicated website "Strategic Communication and Countering Foreign Information Manipulation and Interference" by the European Commission.
[248] European Council, Conclusion of the European Council Meeting of 19 and 20 March 2015, 2015.
[249] For example, the launch of the East StratCom Task Force in 2015 and the Joint Communication on countering hybrid threats (European Commission and High Representative of the Union for Foreign Affairs and Security Policy, A European Union Response, Joint Communication to the European Parliament and the Council, Joint Framework on Countering Hybrid Threats, 2016). See also European Parliament, Resolution of 23 November 2016 on EU strategic communication to counteract propaganda against it by third parties, 2016.

created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm".[250] This definition of disinformation was first encompassed in a Commission Communication on tackling online disinformation[251] in 2018 in which the European Commission supported the development of a "Code of Practice on Disinformation" for online platforms and advertisers. This Communication announced potential regulatory measures in case the Code of Practice on Disinformation should "prove unsatisfactory".[252] The EU Code of Practice on Disinformation was finally published and signed in October 2018.[253] It represented the first time that industry players agreed on a voluntary basis to self-regulatory standards to fight disinformation, moving from mere policy measures to legal ones. Based on the Commission Communication, and in response to the European Council's call for measures to "protect the Union's democratic systems and combat disinformation, including in the context of the upcoming European elections",[254] the European Commission and High Representative of the Union for Foreign Affairs and Security Policy published a Joint Communication on an Action Plan against Disinformation.[255] One of the elements of the Action Plan against Disinformation was the creation of the independent European Digital Media Observatory (EDMO),[256] which serves as a hub for a cross-border and multidisciplinary community of independent fact-checkers, academic researchers and other relevant stakeholders that collaborate with each other. The activities of the EDMO include a mapping of fact-checking organisations and supporting public authorities in the monitoring of the policies put in place by online platforms to limit the spread and the impact of disinformation.

While the Action Plan against Disinformation focused on disinformation in general, the Covid-19 pandemic made the European Commission and High Representative of the Union for Foreign Affairs and Security Policy shift the focus to specific measures in the context of pandemic-related disinformation.[257] Seeking to complement specific measures against disinformation, the European Commission also addressed this topic in other targeted policy instruments such as a European Democracy Action Plan[258] seeking to strengthen democracy by promoting free and fair elections, supporting free and independent media and countering disinformation.

---

[250] European Commission, Tackling Online Disinformation: A European Approach, a Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, COM(2018) 236 final, 26 April 2018.
[251] Ibid.
[252] Ibid, section 3.1.1.
[253] European Commission, Code of Practice on Disinformation, 2018.
[254] European Council, European Council Conclusions, Press release, 18 October 2018.
[255] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Action Plan against Disinformation, a Joint Communication to the European Parliament, the European Council, the Council, the European Economic and Social Committee and the Committee of the Regions, 2018.
[256] The EDMO is managed by a consortium led by the European University Institute in Florence, Italy, and is completely independent from public authorities including the European Commission. For more information, see the dedicate web page.
[257] Tackling COVID-19 Disinformation – Getting the facts right, op. cit., 2020.
[258] European Commission, On the European Democracy Action Plan, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, 2020. This plan also announced the Digital Services Act (DSA) and Transparency and Targeting of Political Advertising (TTPAR) which will be addressed in the following pages.

A first assessment of the implementation of the EU Code of Practice on Disinformation in September 2020 identified several shortcomings[259] and subsequently led to the delivery of a Strengthened Code of Practice on 16 June 2022.[260] On 13 February 2025, the European Commission and the European Board for Digital Services (EBDS)[261] endorsed the integration of the voluntary 2022 Strengthened Code of Practice on Disinformation into the framework of the DSA,[262] which then became the Code of Conduct on Disinformation.[263]

As a consequence, the Code of Conduct on Disinformation serves as a relevant benchmark for assessing DSA compliance related to disinformation risks for providers of very large online platforms (VLOPs) and very large online search engines (VLOSEs),[264] jointly called (VLOPSEs), that follow and uphold its commitments.[265] The commitments are grouped in relation to the following areas: the placing of ads, political advertising, the integrity of users, the empowerment of users, the empowerment of the research community, the empowerment of the fact-checking community, the establishment and maintenance of a transparency centre, the establishment of a permanent task force and the monitoring of the code. For instance, in relation to the placing of ads, the commitments of the signatories include the demonetisation of disinformation (*inter alia*, by ad-tech providers not placing advertisements on websites known to repeatedly spread disinformation) and the prevention of the misuse of advertising systems to disseminate disinformation in the form of advertising messages.[266] As regards the empowerment of the fact-checking community, fact-checking plays an important role in addressing the risks of disinformation and illegal content under the DSA.[267] While the DSA does not mandate fact-checking directly, the EU Code of Conduct recognises fact-checking as a key mitigation measure within the broader framework of systemic risk management and thus requests a commitment to cooperation with the fact-checking community, also in terms of resources and support.[268]

Integrating the Code of Practice on Disinformation into the DSA framework can be seen as an aggravated response to the previous limited commitment and resulting limited effectiveness of the initiatives and actions of VLOPs and VLOSEs.[269]

The Code of Conduct itself does not specify how fact-finding has to be conducted. In order to promote and increase the quality of fact-checking, fact-checking organisations founded the European Fact-Checking Standards Network (EFCSN),[270] an association whose

---

[259] European Commission, Commission Staff Working Document, Assessment of the Code of Practice on Disinformation – Achievements and Areas for further Improvement, SWD(2020) 180 final.
[260] European Commission, Strengthened Code of Practice on Disinformation, 2022.
[261] See Chapter 2.2.2.2.
[262] 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 - DSA), OJ L 277, 27 October 2022.
[263] European Commission, Code of Conduct on Disinformation, 2025.
[264] On the notion of VLOPs and VLOSEs see Chapter 2.2.2.2.
[265] The integration of the Code of Conduct on Disinformation into the DSA framework took effect on 1 July 2025.
[266] European Commission, Code of Conduct on Disinformation, 2025, pp. 10 *et seq*.
[267] Ibid, pp. 37 *et seq*.
[268] Ibid.
[269] Cf. EDMO, *Implementing the EU Code of Practice on Disinformation – An Evaluation of VLOPSE Compliance and Effectiveness (January-June 2024)*, EDMO, Florence, June 2025.
[270] See https://efcsn.com/.

members have committed themselves to certain quality standards outlined in the European Code of Standards for Independent Fact-Checking Organisations.[271] This code constitutes a self-regulatory tool for fact-checkers and provides, *inter alia*, a methodology to verify the accuracy of claims made in the public sphere as well as ethical standards.

Fact-checking has to be distinguished from the concept of "trusted flaggers" regulated under the DSA itself. The latter are designated by national regulators, the Digital Service Coordinators (DSCs), and must meet strict criteria in terms of expertise, independence, transparency and accuracy – their focus is on compliance with the law and not just accuracy or truthfulness; for these reasons they are also attributed a priority status under the notice and actions framework as described above. In contrast, fact-checkers aid platforms to label, contextualise or downgrade false or misleading content rather than request removal. As mentioned above, fact-checking organisations are not a formally defined category in the DSA, but play an important role in risk mitigation.

The integration of fact-checking may at times lead to tensions with the business model of platforms and user dynamics. Thus, social media providers are exploring alternatives such as the "Community Notes"[272] deployed by X that seek to counter disinformation by collaborative fact-checking. The Community Notes programme allows registered users to add context or corrections to potentially misleading posts and are displayed as a note on the original post. This mechanism is subject to the formal proceedings opened against X on 18 December 2023 by the European Commission that focus, *inter alia*, on compliance with the obligations related to countering the dissemination of illegal content in the EU and the effectiveness of measures taken to combat information manipulation on the platform.[273] While the investigation's preliminary findings revealed breaches of DSA obligations, the investigation of, *inter alia*, content moderation is still ongoing in August 2025. In January 2025, the European Commission issued several information requests to X including access requests to application programming interfaces (APIs) to proceed with the complex assessment of systemic risks and their mitigation.[274]

Some insight into content moderation practices is achieved by the mandatory transparency reports to be prepared by all providers of intermediary services which also disclose the number of removal requests, their origin and their handling (see also above). In addition, the DSA transparency database provides for empirical data on the statements of reasons submitted by providers to the Commission. However, aside from offering a summary of the total number of statements submitted, the data provides limited insight into the type of violations, as the most frequently reported category are "other violation of provider's terms and conditions".[275]

---

[271] The European Code of Standards has been published on the EFCSN website.
[272] See https://help.x.com/en/using-x/community-notes.
[273] European Commission, "Commission Opens Formal Proceedings against X under the Digital Services Act", Press release, 18 December 2023.
[274] European Commission, "Commission Addresses Additional Investigatory Measures to X in the Ongoing Proceedings under the Digital Services Act", Press release, 17 January 2025.
[275] Research has shown that more than 99.8% are based on terms of service infringements. See Kaushal R. et al, *Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database* in *The 2024 ACM Conference on Fairness, Accountability, and Transparency (FAccT '24), June 03–06, 2024, Rio de Janeiro, Brazil*, ACM, New York, 2024, pp. 1121-1132.

At the EU level, targeted measures against disinformation can also be seen in specific contexts such as, for instance, the 2024 European elections to the European Parliament, where unprecedented cooperation took place to coordinate responses to foreign information manipulation and interference (FIMI) and disinformation.[276] This included cooperation under specific cooperation structures such as the European Cooperation Network on Elections[277] and several key actions launched to respond to challenges to the integrity of the electoral process which involved collaboration and cooperation between the EU institutions, member states and various entities including the media, fact-checkers and civil society organisations.[278] In April 2024, the activation of the Integrated Political Crisis Response (IPCR) arrangements[279] by the Belgian presidency of the Council provided for rapid and coordinated decision-making at the EU political level, particularly by aiding information exchange among member states and EU institutions in relation to disinformation.[280] This was complemented by monitoring and action through the European Commission's Network against Disinformation (NaD), which, as a deliverable of the Action Plan against Disinformation, constitutes another internal mechanism of the Commission to tackle disinformation.[281] Updates on disinformation narratives being spread in the EU were provided by the EDMO,[282] while further information derived from the reports of providers of online platforms on their measures to protect the integrity of electoral processes based on their commitments under the Code of Practice on Disinformation and reporting obligations under the DSA. Notably, Article 34(1)(c) of the DSA required VLOPSEs to assess and mitigate systemic risks to electoral processes and civic discourse including disinformation risks. Guidance on election-specific risk mitigation measures was also set out in guidelines for providers of VLOPSEs on the mitigation of systemic risks for electoral processes.[283] The DSCs under the DSA also took action, mainly in the form of coordination and stakeholder engagement in their national contexts complementing the work of the European Commission.[284] As regards the Code of Practice on Disinformation, the signatories also established a Rapid Response System (RRS) which allowed non-platform participants

[276] See European Commission, *Report on the 2024 Elections to the European Parliament*, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Com(2025) 287 final, 2025.
[277] See European Commission, Terms of Reference, European Cooperation Network on Elections.
[278] See ibid, pp. 13 *et seq.*
[279] European Commission, Council Implementing Decision (EU) 2018/1993 of 11 December 2018 on the EU Integrated Political Crisis Response Arrangements OJ L 320/28, 17 December 2022. These arrangements provide a flexible crisis mechanism supporting the presidency of the Council of the EU in dealing with major natural or man-made cross-sectorial disasters.
[280] Council of the EU, "Foreign Interference: Presidency Reinforces Exchange of Information ahead of the June 2024 European Elections", Press release, 24 April 2024.
[281] European Commission, Report on the 2024 Elections to the European Parliament, Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Com(2025) 287 final, 2025, p. 13.
[282] See EU Elections Disinfo Bulletin at EU Elections Disinfo Bulletin – EDMO.
[283] European Commission, Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, [2024] OJ C 2024/3014. On the election guidelines see also EBDS, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, Publications Office of the European Union, Luxembourg, 2024, p. 11.
[284] EBDS, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, pp. 13 *et seq.*

to quickly contribute information that they consider potentially harmful to the integrity of electoral processes, thereby helping to achieve a full picture of disinformation campaigns.[285]

In sum, the self-regulatory commitments and the obligations for providers of VLOPSEs, cooperation under specific cooperation structures, easier information exchange and increased information gathering complemented by several table-top exercises have been perceived by EU institutions to have resulted in increased preparedness and to have facilitated the detection of risks.[286] These measures are now increasingly complemented by hard law specifically addressing disinformation. One such law is the new Regulation on Transparency and Targeting of Political Advertising (TTPAR),[287] which provides for EU common standards addressing certain problematic practices in the dissemination of political advertising in the EU, including funding from outside the EU. In addition, accelerated regulatory cooperation under the European Media Freedom Act (EMFA) aims to facilitate a quick response to foreign disinformation by "rogue media services" threatening the public security of a member state.[288] It remains to be seen to what extent member states will prefer to choose the EMFA's option to block non-European media services within the EU via national measures taken by media authorities under the coordination of the newly introduced European Board for Media Services (EBMS), or via sanctions imposed by the Council of the EU.

3.2. The example of Romania

Dr Roxana Radu, Associate Professor of Digital Technologies and Public Policy, Blavatnik School of Government, University of Oxford

3.2.1. National legal framework concerning platforms

The influence of online platforms on the daily life of Romanians is significant. Dependence on Facebook, WhatsApp, YouTube and TikTok as primary sources of information (including for news) is very high.[289] In a country with one of the lowest digital literacy rates in

[285] The actors involved detected and exposed various attempts to mislead voters with disinformation, for example, by false information about how to vote and false information on European policies. See European Commission, "European Elections: EU Institutions Prepared to Counter Disinformation", Press release, 5 June 2024.

[286] European Commission, Report on the 2024 Elections to the European Parliament, op. cit., p. 15; EBDS, *Report on the European Elections, Digital Services Act and Code of Practice on Disinformation*, 2024, pp. 18 *et seq.*

[287] Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L 2024/900, 20 March 2024.

[288] Articles 13(l) and 17 EMFA. For an overview on how the EMFA and TTPAR complement the "disinformation" strategy of the EU see Eskens S., "The Role of Regulation on the Transparency and Targeting of Political Advertising and European Media Freedom Act in the EU's Anti-Disinformation Strategy", *Computer Law & Security Review*, 58 - 106185, 2025.

[289] Reuters Institute for the Study of Journalism, *Digital News Report 2025 – Romania*, 2025.

Europe,[290] the propagation of fake news and disinformation reached a first peak during the Covid-19 pandemic[291] and has persisted in shaping public opinion, culminating in the 2024 annulment of the presidential elections.

Romania's online platform approach harmonises national legislation with European Union legal acts, aimed at establishing a cohesive Digital Single Market. Online platforms are required to comply with domestic provisions, such as *Lege nr. 365/2002 privind comerțul electronic* (Law on electronic commerce), which sets out foundational rules for online transactions, as well as EU-wide regulations like the GDPR[292] or the DSA, which aim to safeguard users' fundamental rights by imposing obligations on platforms for transparency, accountability, and compliance.

As detailed in Chapter 2 of this publication, the DSA introduces obligations for intermediaries. For VLOPSEs, the European Commission serves as the competent authority, working closely with nationally designated Digital Services Coordinators. In Romania, this role falls to the National Authority for Management and Regulation in Communications (ANCOM).

The other relevant authority is the National Audiovisual Council (CNA), which in the 2025 assessment by the European Commission continues to "lack sufficient staff and technological resources to fulfil its mandate, especially in light of the implementation of the Digital Services Act".[293] The mandate of the CNA was expanded by the transposition of the EU Audiovisual Media Services Directive (AVMSD)[294] into national law and related amendments to *Lege nr. 504/2002 Legea audiovizualului* (Audiovisual Law No. 504/2022) and the *Ordonata Guvernului nr. 39/2005 privind cinematografia* (Cinematography Ordinance No. 39/2005). These changes oblige streaming platforms (video-on-demand providers) to contribute a part of their local revenues, either through levies or by investing in the national film industry, under defined conditions.[295]

Beyond regulatory alignment with the EU, initiatives focused on public awareness and high-quality online content have been very limited. Digital literacy programmes, independent fact-checking, and funding for public research and local journalism have not

[290] TRIO Project, *Romania National Report Summary*, March 2023; Issue Monitoring, *Romania's Digital Environment: Navigating the Path to a Tech-Driven Future*, 23 August 2024.
[291] EU DisinfoLab, *Disinformation Landscape in Romania*, September 2023.
[292] European Commission, General Data Protection Regulation, 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, OJ L 119, 4 May 2016.
[293] European Commission – Resource Centre on Media Freedom, 2025 Rule of Law Report – Country Chapter: Romania, July 2025.
[294] 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), OJ L 303, 28 November 2018.
[295] Cristian D., "Romania Imposes Financial Contributions on Streaming Platforms to Support National Film Fund", *Business Review*, 17 October 2022.

been prioritised, leaving societal resilience underdeveloped and both the supply of and demand for disinformation largely unaddressed.[296]

3.2.2. Specific rules regarding disinformation

The surge of online disinformation became particularly evident during the Covid-19 pandemic, when the presidential decree declaring a state of emergency empowered the government to take any measures deemed necessary to curb the spread of false information — including the authority to shut down sources of fake news, via ANCOM.[297] Citizen susceptibility to the Covid-19 "infodemic"[298] in Romania was among the highest in Europe, as evidenced by widespread belief in conspiracy theories and low vaccination rates.[299] In that context, the Romanian Senate adopted Decision No. 24 on the European Commission's Communication on Tackling Covid-19 disinformation – Getting the facts right.[300/301] However, its recommendations have not resulted in concrete actions to increase resilience to disinformation. A 2022 report by the Euro-Atlantic Resilience Centre noted that Romania's legal and institutional tools were "imperfectly suited to the current phase of technological development […]. Legal provisions and relevant institutions did not cover the whole spectrum of threats or allow for a quick and efficient counteraction".[302]

In the national context, countering disinformation consists of: 1) broader legal safeguards that apply in general terms; 2) more targeted, strategic efforts to address the new challenges; and 3) implementation of broader EU initiatives. At the foundational level, existing provisions within the Penal Code and constitutional guarantees offer broad-spectrum protections against the spread of false or misleading information. Article 404 of the Penal Code (updated) makes it a crime to knowingly spread false information that

---

[296] Cercelescu M., *Dezinformarea în epoca post-adevăr. Avem, în România, legislație sau alte măsuri pentru combaterea dezinformării?*, JURIDICE.ro, 1 March 2019; Munteanu D., *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.

[297] *Decree on the Establishment of the State of Emergency in the Territory of Romania*, Official Gazette of Romania, Part I, No. 212/16, March 2020.

[298] Radu R., "Fighting the 'Infodemic': Legal Responses to COVID-19 Disinformation", *Social Media + Society*, 6(3), 2020.

[299] Mosila A., "The Challenge of Populism and Disinformation on the Pandemic Response in Romania", *EuropeNow Journal*, 20 November 2023.; Cucu C., "Disinformation Landscape in Romania", EU DisinfoLab, September 2023.

[300] European Commission and High Representative of the Union for Foreign Affairs and Security Policy, Joint Communication to the European Parliament, the European Council, the European Economic and Social Committee and the Committee of the Regions: Tackling COVID-19 Disinformation – Getting the facts right (2020).

[301] Romanian Senate, *Hotărâre nr. 24 din 8 martie 2021referitoare la Comunicarea Comisiei către Parlamentul European, Consiliu, Comitetul Economic și Social European și Comitetul Regiunilor – Combaterea dezinformării în legătură cu COVID-19 – Asigurarea unei informări corecte – JOIN(2020) 8 final* (Decision No. 24 of 8 March 2021, regarding the Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions: Tackling COVID-19 Disinformation – Getting the facts right), 25 March 2021.

[302] Munteanu, D., *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.

threatens national security, punishable by one to five years in prison.[303] In practice, however, applying this provision to sophisticated forms of disinformation is difficult. First, disinformation does not always consist of fabricated content — it can stem from genuine content that has been manipulated or taken out of context, imposter content or false connections.[304] Second, citizens themselves are often vulnerable to such content and may share it further without realising its potential national security implications.[305] About a quarter of Romanian users of online platforms also report sharing news via social media, messaging or email.[306]

The Romanian Constitution sets out provisions on freedom of expression and the right to information, holding publishers, producers, authors, or broadcasters liable for published content and requiring mass media to ensure accurate public information. Yet modern disinformation challenges this framework: harm is often diffuse, affecting the public at large rather than identifiable individuals, via obscure networks that keep changing forms. Recognising the scale of the problem, Romania has included an anti-disinformation plan in its National Defence Strategy for 2020–2024, but its implementation schedule (since 2021) has remained a classified document.[307] Among the targeted efforts being pursued, the Ministry of Defence has spoken publicly about countering disinformation via the InfoRadar platform, which monitors false information and disinformation campaigns on topics of interest to the army, and offers citizens the possibility of reporting relevant cases through a contact form. The Ministry of Digitalisation has also set up a contact point for election-related deepfake reporting, as the draft bill requiring deepfake content to carry broadcast warnings is still pending final approval.[308]

Romania also participates in the wider EU framework addressing disinformation and democratic processes. Following the *Ordonanţă de Urgenţă nr. 6/2019* (Emergency Ordinance No. 6/2019), the Permanent Electoral Authority (AEP) was designated as the single point of contact for all cybersecurity incidents and disinformation campaigns in the context of the European Parliamentary elections. In 2024, the AEP published a guide for preventing and combatting disinformation among voters, explaining how disinformation works, providing tools to identify and analyse false content, and offering recommendations for journalists, content creators, and electoral competitors.[309] Despite these efforts, regulatory enforcement remained limited until the CNA and ANCOM formally alerted the European Commission to significant irregularities in TikTok's management of political content during

[303] *Codul Penal din 17 Iulie 2009* (Penal Code, Law No. 286/2009), updated as of 5 February 2017.
[304] United Nations Office of the High Commissioner for Human Rights (OHCHR), Report on Disinformation, A/HRC/47/25, 2021.
[305] Munteanu D., *Barometrul rezilienței societale la dezinformare*, Centrul Euro-Atlantic pentru Reziliență (E-ARC), Bucarest, 2022.
[306] Reuters Institute for the Study of Journalism, *Digital News Report 2025 – Romania*, 2025.
[307] Stanoiu I., "*Serviciile de informații, Administrația Prezidențială și guvernul au scris și țin la secret planul național anti-dezinformare, care a eșuat*,", *Context.ro*, 5 February 2025.
[308] *Legislative Proposal L295/2023, Propunere legislativă privind interzicerea utilizării malițioase a tehnologiei și limitarea fenomenului Deepfake* (Proposal to ban the malicious use of technology and limit the deepfake phenomenon).
[309] Permanent Electoral Authority (AEP), Ghid de prevenire și combatere a acțiunilor de dezinformare a alegătorilor, March 2024.

the presidential elections in November 2024,[310] prompting the launch of an official investigation by the European Commission under the DSA on 17 December 2024.[311]

3.2.3. The annulment of Romania's 2024 presidential election

The online space became the battleground for electoral integrity long before voters reached the polls on 24 November 2024 for the presidential election. Disinformation played a key role in compromising the electoral process, building on deeper structural vulnerabilities, including political instability, economic uncertainty, and societal polarisation. Socio-economic and political fault lines, long present, became sharply visible in online discourse.[312] In the presidential contest, Călin Georgescu, a candidate with a pro-Russian agenda, unexpectedly rose to first place during the first ballot, despite having only 6% support in pre-election polls. This surge was facilitated by opaque campaign financing,[313] the use of digital influencers, and the recommender system of Tik Tok,[314] a platform with 9 million Romanian users. In response to credible reports of foreign interference and electoral irregularities,[315] the Constitutional Court concluded that the integrity of the entire electoral process had been compromised, annulled the results and ordered a re-run of the election.[316] Georgescu was subsequently barred from standing again.[317]

The cancellation of the vote showed that all the national measures to protect the electoral processes had fallen short in practice. At the European level, the standards set out in the Commission's 2024 Guidelines for the mitigation of systemic risks for electoral processes[318] were not fulfilled. Large platforms took insufficient measures to address threats in real time, raising questions about their accountability. In Romania, TikTok did not enforce its own ban on political advertising,[319] allowing accounts and election-related content to be aggressively promoted. Despite repeated notifications from national authorities about electoral irregularities,[320] the platform failed to act.

---

[310] Digital Policy Alert, "Romania: Announced NAC and ANCOM Referral to the European Commission for an Investigation into TikTok for Alleged Failure to Address Disinformation and Electoral Manipulation Amplification under DSA", *Digital Policy Alert*, 26 November 2024.
[311] European Commission, Commission Opens Formal Proceedings Against TikTok on Election Risks under the Digital Services Act", Press release, 17 December 2024.
[312] Radu R., "TikTok, Telegram, and Trust: Urgent Lessons from Romania's Election", TechPolicy Press, 25 June 2025.
[313] Romanian Presidential Administration, Document CSAT SRI I, 4 December 2024.
[314] EDMO (European Digital Media Observatory), Analysis of the 2024 Romanian Presidential Elections: The Role of Social Media and Emerging Political Trends, 26 November 2024.
[315] Romanian Presidential Administration, Document CSAT SRI I, 4 December 2024.
[316] Constitutional Court of Romania, Press release, 6 December 2024.
[317] Rainsford S. and Gozzi L., "Final ruling bars far-right Georgescu from Romanian vote", *BBC News*, 11 March 2025.
[318] European Commission, Commission Guidelines for Providers of Very Large Online Platforms and Very Large Online Search Engines on the Mitigation of Systemic Risks for Electoral Processes pursuant to Article 35(3) of Regulation (EU) 2022/2065, (C/2024/3014), 26 April 2024.
[319] TikTok, TikTok Ads Policy – Politics, Government, and Elections, last updated July 2025.
[320] DIGI24, "*ANCOM: TikTok nu a acționat la solicitarea AEP ce semnala diverse nereguli legate de conținutul ilegal distribuit*" *Digi24*, 26 November 2024.

The Romanian vote annulment case also shows the evolving character of disinformation, which moved fluidly between influencers, monetisation tools, and algorithmic promotion of electoral content.[321] With its low digital literacy, political and economic instability, and widespread voter dissatisfaction, the country was unprepared to counter disinformation at scale. Legislative inertia and limited institutional capacity further compounded the problem, creating conditions that allowed misleading information to spread unchecked. The above-mentioned investigation, launched by the European Commission in December 2024, into TikTok's policies on political ads, paid political content, and the role of its recommender systems in amplifying such material – is still underway.[322] Evidence collection has been slow, in part because the DSA lacks deadlines for concluding formal proceedings. Only the European Commission can assess compliance by VLOPs, relying on cooperation with Ireland's *Coimisiún na Meán*, given TikTok's EU headquarters in Ireland.

At the national level, two legislative responses emerged. On 16 January 2025, the government issued Emergency Ordinance No. 1/2025,[323] which changed political advertising rules without consulting stakeholders.[324] The ordinance required all electoral content, including that from private citizens, to be properly labelled. In March 2025, a draft law on curbing online disinformation and harmful content was tabled and subsequently passed by the Romanian Senate in June 2025.[325] The draft law introduces stricter rules for VLOPs than those set out in the DSA. In its current form – due to be discussed by the Chamber of Deputies in the coming months – it requires platforms to limit the spread of potentially harmful content to no more than 150 users, prohibit its promotion, and remove illegal content within 15 minutes of publication when classifying it through automated systems. It also bans paid promotion of content inciting hate, violence, or national-interest disinformation. Failure to act effectively – measured by a 30% threshold of validated user reports – would result in fines of 1% of turnover enforced by ANCOM. While the law seeks to strengthen public protection, its broad definition of harmful content, heavy reliance on artificial intelligence (AI), and accelerated timelines raise concerns over feasibility and risks to freedom of expression, as experts have cautioned.[326] It marks a significant expansion beyond the obligations imposed by the DSA and can set a precedent, if approved.

[321] Ings R., "The TikTokers accused of triggering an election scandal", *BBC News*, 30 April 2025.
[322] European Commission, "Commission Opens Formal Proceedings Against TikTok on Election Risks under the Digital Services Act", Press release, 17 December 2024.
[323] Emergency Ordinance No. 1/2025 on certain measures for the organisation and conduct of the 2025 elections for the President of Romania and the 2025 local by-elections, 17 January 2025.
[324] Funky Citizens, "Romania's Elections Overview, 22 April 2025", *European Digital Media Observatory*, 22 April 2025.
[325] Mocanu R., "*A fost adoptata de Senat legal impotrivata manipularii online propusa de USR*", *MediaFax*, 16 June 2025.
[326] CMS LawNow, "Romania proposes stricter rules against harmful content on social media", *CMS LawNow*, 10 March 2025.

3.3. The example of France

Dr William Gilles, Associate Professor, University of Paris 1 Panthéon Sorbonne and Dr Irène Bouhadana, Associate Professor, University of Paris 1 Panthéon Sorbonne

3.3.1. National legal framework concerning platforms

The national law in France governing platforms is primarily framed by constitutional case law, which specifies the procedures under which French lawmakers may take measures relating to such platforms. Thus, in its decision relating to the Law promoting the dissemination and protection of creative works on the Internet (known as Hadopi 1),[327] the Constitutional Council ruled that freedom of communication and expression, as provided for in Article 11 of the Declaration of the Rights of Man and of the Citizen of 26 August 1789,[328] "implies freedom of access" to "online public communication services", and therefore to the Internet.[329]

In its 2020 decision relating to the law aimed at combatting hateful content on the Internet (known as the Avia Law),[330] the Constitutional Council reiterated this case law, specifying that freedom of communication and expression also implies the freedom to express oneself.[331] It therefore ruled that

> *given the current state of communication technology and the widespread development of online public communication services, as well as the importance of these services for participation in democratic life and the expression of ideas and opinions, this right implies the freedom to access these services and to express oneself on them.*

It added that the French legislature may adopt a legal framework aimed at putting an end to abuses of freedom of expression and communication that undermine public order and the rights of third parties, by classifying, for the first time, as belonging to such a category of abuses the dissemination of pornographic images depicting minors and incitement to acts of terrorism or their glorification.

However, the Constitutional Council's decision in 2020 struck down several provisions of the Avia Law on the grounds that the infringements on freedom of expression and communication were not appropriate, necessary, or proportionate to the objective pursued. The provisions invalidated would have allowed the competent administrative authority to require hosting providers or publishers of an online communication service to remove content that constitutes child pornography or incites or glorifies acts of terrorism,

---

[327] Légifrance, *Loi n° 2009-669 du 12 juin 2009, favorisant la diffusion et la protection de la création sur internet*, *Journal officiel de la République française* (JORF) No. 0135 of 13 June 2009 (Hadopi).
[328] *La déclaration des droits de l'homme et du citoyen* (Official English translation).
[329] *Conseil Constitutionnel*, Decision No. 2009-580 of 10 June 2009.
[330] *Loi n° 2020-766 visant à lutter contre les contenus haineux sur internet*, JORF No. 0156 of 25 June 2020 (Avia Law).
[331] *Conseil Constitutionnel*, Decision No. 2020-801 DC of 18 June 2020.

and, if such content had not been removed within 24 hours, to order access providers to immediately block access to such content. However, the Constitutional Council considered, first, that the unlawful nature of such content would not depend on its explicit expression but solely on the assessment of the administration. Second, an appeal against a request for removal would not have suspensive effect: the publisher or hosting provider would only have one hour to block access to the content, a time frame so short that it would prevent them from obtaining a court ruling prior to removing the offending content, while they would face a fine of EUR 250 000 and a one-year prison sentence if they failed to remove the content within this time frame. Similarly, the Constitutional Council also struck down the provisions of the law that required online platform operators, in order to avoid criminal penalties, to remove and prevent access within 24 hours to "content that is manifestly illegal due to its hateful or sexual nature".

The remaining provisions of the law, which, after being reviewed by the Constitutional Council, became the Avia Law as mentioned above, aimed at combatting hateful content on the Internet. This law amended the *Code de l'éducation* (Education Code)[332] in order to strengthen the education of students and their teachers regarding the use of digital tools and resources, with a view to preventing the dissemination of hateful content online and developing digital citizenship. The Avia Law also created the Online Hate Observatory,[333] attached to the French Audiovisual and Digital Communication Regulatory Authority (ARCOM),[334] which is an independent French public authority responsible for guaranteeing freedom of communication. Operational since 2020, this observatory's mission is to monitor and analyse hateful content online. It comprises four colleges: administrations, researchers, associations, and operators, the latter bringing together Dailymotion, Facebook, Google, LinkedIn, Microsoft, Qwant, Snapchat, TikTok, Twitch, X (formerly Twitter), Wikimedia France, and Yubo. Finally, the Avia Law amended the *Loi pour la confiance dans l'économie numérique* (Law on confidence in the digital economy – LCEN Law),[335] which is the French legislation of reference concerning the legal framework for Internet actors. This text was amended by the *Loi visant à sécuriser et à reguler l'espace numérique* (Law aimed at securing and regulating the digital space – SREN Law),[336] in particular, to adapt French law to European Union law following the adoption of the DMA and the DSA. It was amended more recently by the *Loi visant à sortir la France du piège du narcotrafic* (Law aimed at freeing France from the trap of drug trafficking)[337] to include these issues. At the same time, it was specified that the main purpose of this legislation is not to regulate platforms.

[332] Légifrance, *Code de l'éducation*.
[333] See ARCOM, *"Observateur de la haine en ligne : analyser pour mieux lutter"*.
[334] See *Autorité de régulation de la communication audiovisuelle et numérique (ARCOM) website*.
[335] Légifrance, *Loi n° 2004-575 du 21 juin 2004, pour la confiance dans l'économie numérique,* JORF No. 0143 of 22 June 2004.
[336] Légifrance, *Loi n° 2024-449 du 21 mai 2024, visant à sécuriser et à réguler l'espace numérique,* JORF No. 0117 of 22 May 2024.
[337] Légifrance, *Loi n° 2025-532 du 13 juin 2025, visant à sortir la France du piège du narcotrafic*, JORF No. 0137 of 14 June 2025.

Finally, with regard to platform regulation, Decree No. 2020-1102 of 31 August 2020[338] creates, within the Directorate-General for Enterprise, under the authority of the Ministries of Economy, Culture, and Digital Affairs, a national service called the *Pôle d'Expertise de la Régulation Numérique* (Center of expertise for digital platform regulation – PEReN), whose role is to provide expertise and technical assistance to government agencies and independent authorities responsible for regulating digital platforms. Decree No. 2022-603 of 21 April 2022,[339] amended by Decree No. 2025-385 of 28 April 2025,[340] specifies which independent administrative and public authorities are eligible to bring matters to PEReN, namely: the Competition Authority (ADLC), the Financial Markets Authority (AMF), the National Gaming Authority (ANJ), the Regulatory Authority for Electronic Communications, Postal Services and Press Distribution (ARCEP), ARCOM, the Transport Regulatory Authority (ART), the Energy Regulatory Commission (CRE), the National Commission for Information Technology and Civil Liberties (CNIL), and the Ombudsman.

3.3.2 Specific rules regarding disinformation

The advent of the data society and the development of platforms have highlighted the risks posed by new technologies in terms of the spread of fake news, and France is no exception to this new context. This awareness was particularly evident during the 2017 French presidential elections, with the emergence of foreign interference posing risks to the proper organisation of the elections. This context prompted the French legislature to adopt its first legislation on false information, with the specific aim of combatting false information during elections, with the adoption of the *Loi n° 2018-1202 relative à la lutte contre la manipulation de l'information* (Law No. 2018-1202 on combatting the manipulation of information).[341] This legal framework was subsequently amended, in particular by the SREN Law, which implements the DSA into French law, with direct application, and designates ARCOM as the coordinator of digital services. The legal framework currently applicable to limiting the spread of false information is thus as follows.

First, the French Electoral Code[342] has been amended to ensure greater integrity in French elections and limit the risk of foreign interference in this area. In its latest version, Article L163-1 of the Electoral Code requires very large online platforms and search

[338] Légifrance, *Décret n° 2020-1102 du 31 août 2020*, portant création d'un service à compétence dénommé "Pôle d'expertise de la régulation numérique", JORF No. 0214 of 2 September 2020.
[339] Légifrance, *Décret n° 2022-603 du 21 avril 2022, fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation*, JORF No. 0095 of 23 April 2022.
[340] Légifrance, *Décret n° 2025-385 du 28 avril 2025, complétant le décret n° 2022-603 du 21 avril 2022 fixant la liste des autorités administratives et publiques indépendantes pouvant recourir à l'appui du pôle d'expertise de la régulation numérique et relatif aux méthodes de collecte de données mises en œuvre par ce service dans le cadre de ses activités d'expérimentation*, JORF No. 0102 of 30 April 2025.
[341] Légifrance, *Loi n° 2018-1202 du 22 décembre 2018, relative à la lutte contre la manipulation de l'information*, JORF No. 0297 of 23 December 2018.
[342] Légifrance, *Code électoral*.

engines, as defined by the DSA, to be transparent when disseminating information relating to debates of general interest. Thus, in the three months preceding the elections and until the day they are won, they must communicate, in the register provided for in Article 39 of the DSA, fair, clear, and transparent information concerning not only the sponsors of the promotion of content relating to these debates of general interest, but also the manner in which personal data is used in this context. They must also indicate in this register the amounts they have received in the event of remuneration exceeding €100 (excluding tax) per piece of information content disseminated in the context of the debate of general interest. These provisions are among those imposing a duty of cooperation on online platforms with regard to the dissemination of false information. They are in addition to the rules laid down by the DSA concerning the general obligations of platforms, including outside election periods, such as those relating to the transparency of their recommendation systems.

For its part, Article L163-2 of the Electoral Code establishes the possibility for a candidate, the public prosecutor, a party, or any person with an interest in taking action to refer the matter to a judge in summary proceedings during the same election period in the event of deliberate, artificial, or automated and massive online dissemination of information alleging or imputing inaccurate or misleading facts likely to undermine the integrity of the elections. The magistrate then has 48 hours to issue a ruling, with the appeal judge subject to the same time limit; the aim is to ensure a quick response to the dissemination of false information likely to influence the election result.

More generally, lawmakers sought to include an educational component in the fight against disinformation, and with this in mind amended the Education Code[343] to train primary school (Article L312-5) and middle school students (Article L332-5) in critically analysing and verifying the reliability of information available in the media, as well as teachers who are responsible for providing this education (Article L721-2). Radio and audiovisual media and VSP providers are required to contribute to this educational objective by taking measures to this end (Articles 28, 43-11, and 60 of *Loi n° 86-1067 du 30 septembre 1986 relative à la liberté de communication* – Law of 30 September 1986 on freedom of communication, known as the Léotard Law).[344]

In addition, the Léotard Law grants ARCOM powers to combat the dissemination of false information. Article 17-2 of this law reiterates its role in this area when such dissemination may disturb public order or affect the integrity of elections.

The Léotard Law also allows ARCOM to take action against audiovisual communication services that have signed an agreement with this authority, which are controlled or influenced by a foreign state and which deliberately broadcast false information. If such information is likely to affect the integrity of the election in the three months preceding an election and until the day on which the election is conducted (Article 33-1-1), ARCOM may suspend or cease such broadcasting as a preventive measure or to put an end to the resulting disturbance. If false information is likely to harm the fundamental

[343] Légifrance, *Code de l'education*.
[344] Légifrance, *Loi n° 86-1067 du 30 septembre 1986*, *relative à la liberté de communication,* JORF of 1 October 1986.

interests of the nation, and for example hinders the proper functioning of institutions, ARCOM may, after formal notice, unilaterally terminate this agreement (Article 42-6). If it finds a breach of the obligations provided for by the Léotard Law, which includes those examples mentioned above, the President of ARCOM may also refer the matter to the Council of State for summary proceedings to obtain an order regarding the immediate enforcement of measures to ensure compliance, the cessation of the irregularity, or the removal of its effects (Article 42-10). More generally, ARCOM may refer the matter to the public prosecutor when it finds a violation of the Léotard Law.

ARCOM is also responsible, in accordance with Article 58 of the Léotard Law, for ensuring that online platform operators comply with their obligations as set out in the LCEN Law. With regard to combatting the manipulation of information that could disturb public order or alter the integrity of elections, ARCOM makes recommendations on this subject to major online platform providers, major search engines, and major VSP service providers, and periodically publishes a report on the measures they have taken. Finally, it is responsible for ensuring that online platforms comply with the rules on combatting hateful content (Article 62).

Outside of this context, French lawmakers have not adopted specific legal rules for other cases involving the dissemination of false information. With regard to the dissemination of information online, it is important to note that French lawmakers have affirmed the principle of freedom of electronic communication to the public, with any restrictions falling within the scope of the exceptions provided for by the Léotard Law. Among the limitations mentioned, it is nevertheless possible to submit an appeal against misinformation, invoking several scenarios provided for in Article 1 of the Léotard Law, and more particularly, the need to uphold human dignity, freedom, pluralism of thought and opinion, and public order, and even to protect children and adolescents when they are targeted.

In addition, several provisions of the *Loi du 29 juillet 1881 sur la liberté de la presse* (Law of 29 July 1881 on freedom of the press)[345], while not specifically targeting false information, nevertheless may be applied to sanction its consequences. In criminal terms, disinformation could be punished under several crimes and offences provided for by this law. Three situations are particularly illustrative in this context.

On the one hand, false information could lead to incitement to commit crimes and offences punishable by up to five years' imprisonment and a fine of EUR 45 000, in accordance with Articles 24 and 24 bis of the Law on freedom of the press. In other words, in this case, it would be a situation in which the commission of a crime or offence was directly provoked by false information. By way of illustration, in a ruling dated 15 October 2019,[346] the Court of Cassation had to rule on stigmatising messages concerning the supposed origin or religion of individuals and equating religious affiliation with a pathology. This false information, which had been disseminated on Twitter and Facebook, was classified as racial insults and incitement to discrimination, hatred, or violence, justifying the conviction of its author under Articles 24 and 27 of the aforementioned law,

[345] Légifrance, *Loi du 29 juillet 1881, sur la liberté de la presse*.
[346] *Court du Cassation*, *Décision n° 18-85.365* (not published in the official law reports).

insofar as, according to the judges, these "comments explicitly or implicitly urged the public to discriminate against groups of people targeted because of their race or religion".

On the other hand, false information could also be punished as a crime against the persons mentioned in Article 29 of the Law on freedom of the press, when it takes the form of insults, or, in other words, contempt, baseless contempt or invective (penalties ranging from €12 000 to €75 000), or defamation. The latter case would result from disinformation aimed at alleging or imputing a fact that damages the honour of a person or their reputation or the body to which they belong. The perpetrator could then face a fine ranging from €12 000 to €45 000 depending on the circumstances, with the most severe penalties applying in particular to defamation against courts, public administrations, civil servants, citizens in charge of a public service or public office, the President of the Republic, or on the grounds of their origin, membership or non-membership of a particular ethnic group, nation, race, or religion. In France, a recent example involved the online dissemination of false information that went viral, claiming that Brigitte Macron, the wife of the President of the French Republic, was a transgender woman who had undergone several surgical procedures for this purpose. Initially convicted of defamation on 12 September 2024, by the Paris Judicial Court, the authors of this false information were subsequently acquitted by the Paris Court of Appeal on 10 July 10 2025, on the grounds of their "good faith". This legal proceeding is currently pending, as an appeal has been filed with the Court of Cassation.[347]

Finally, Article 27 of the Law on freedom of the press provides for a fine of €45 000 against any person who publishes, disseminates, or reproduces false news to a third party, with this fine being increased to €135 000 if the discipline or morale of the armed forces, as well as the nation's war effort, are targeted. However, this scenario concerns a specific case, since in order to be characterised as such, the publication, dissemination, or reproduction must have been carried out in bad faith and must have caused or risked a disturbance to public order. This last scenario highlights the need to clarify the distinction between the concept of false information and that of "fake news". Examining the bill on the dissemination of false information – subsequently adopted as Law No. 2018-1202 of 22 December 2018 on combatting the manipulation of information[348] – the Council of State considered it useful, in an advisory opinion dated 4 May 2018, to clarify the distinction between the concept of false information and that of "fake news", which already existed in French law through the Law on freedom of the press, as well as in the Electoral Code.[349] It points out that, according to the case law of the Court of Cassation, fake news is based on "a specific and detailed fact, not yet disclosed and whose false nature is established objectively", whereas false information has a broader scope, as this concept does not include the condition of "no prior disclosure of the disputed information". In addition, the Council of State recommended limiting the concept of false information to information disseminated with "a deliberate intention to cause harm".

[347] Le Monde with AFP, "Brigitte Macron Takes Gender Libel Case to France's Highest Appeals Court", *Le Monde*, 14 July 2025.
[348] op. cit.
[349] Conseil d'État, *Lutte contre les fausses informations, avis consultatif*, 4 May 2018.

3.3.3 Application in the case of elections

The geopolitical context of recent years and the increase in foreign interference have made it clear that the fight against false information cannot rely solely on previously mentioned Law No. 2018-1202 on combatting the manipulation of information, prompting lawmakers to take new measures in 2024 to achieve this goal by using algorithms based on the algorithmic processing that had been implemented on an experimental basis by the Law on intelligence to identify terrorist threats.[350] Introduced in Article L851-3 of the Internal Security Code,[351] this measure was extended twice before being made permanent by the Law on the prevention of terrorist acts and intelligence.[352] The law aimed at preventing foreign interference in France[353] sought to extend this measure by allowing the deployment of this algorithmic processing to identify, based on connection data and the addresses of the Internet content consulted, any foreign interference or attempted interference. In return, procedural safeguards are established by requiring an authorisation by the prime minister respecting the principle of proportionality and precisely defining the authorised processing; the government must also submit a report to parliament on the implementation of this legislative provision.

In addition to this legal framework, France also took action at the operational level by setting up a service to monitor and protect against foreign digital interference (VIGINUM). This service, which has national jurisdiction, was created by Decree No. 2021-922 of 13 July 2021,[354] and is attached to the General Secretariat for Defence and National Security (SGDSN). VIGINUM's mission is to detect and characterise foreign digital interference operations disseminated publicly on online platforms, particularly during election periods, when they are likely to alter the way citizens are informed. The information threats targeted specifically concern operations directly or indirectly linked to a foreign state or a foreign non-state entity that consist of deliberately disseminating false information on a massive scale, through artificial or automation processes using an online public communication service. The concept of false information refers in this context to the description given in Article R*1132-3 of the Defence Code[355] of such operations, namely "allegations or imputations of facts that are manifestly inaccurate or misleading and likely to harm the fundamental interests of the Nation". Finally, VIGINUM provides support to several French institutions: assistance to the SGDSN in coordinating and leading interministerial efforts to combat fake news; contributions to European and international efforts in this area; and the provision of information to ARCOM and the National

[350] Légifrance, *Loi n° 2015-912 du 24 juillet 2015*, relative au renseignement, JORF No. 0171 of 26 July 2015.
[351] Légifrance, *Code de la sécurité intérieure*.
[352] Légifrance, *Loi n° 2021-998 du 30 juillet 2021*, relative à la prévention d'actes de terrorisme et au renseignement, JORF No. 0176 of 31 July 2021.
[353] Légifrance, *Loi n° 2024-850 du 25 juillet 2024*, visant à prévenir les ingérences étrangères en France, JORF No. 0177 of 26 July 2024.
[354] Légifrance, *Décret n° 2021-922 du 13 juillet 2021 portant création, auprès du secrétaire général de la défense et de la sécurité nationale, d'un service à compétence nationale dénommé « service de vigilance et de protection contre les ingérences numériques étrangères »*, JORF No. 0162 of 14 July 2021.
[355] Légifrance, *Code de la défense*.

Commission for the Control of Election Campaigns in their respective roles in combatting these threats.

3.4. The example of Ukraine

Dr Dariia Opryshko, NGO Human Rights Platform

3.4.1. National legal framework concerning platforms

For a long time in Ukraine, issues relating to online platforms and the publication of content were regulated by general provisions in various legislative acts. Ukrainian legislation permitted the blocking of content in cases concerning the dissemination of content depicting the sexual abuse of children or the violation of copyright and related rights.[356]

The first specific provisions aimed at regulating online platforms in Ukraine were introduced by the Ukrainian Media Law (UML).[357] Adopted on 13 December 2022, this law came into force on 31 March 2023. The UML distinguishes between video-sharing platforms (VSPs) and shared access to information platforms[358] (online platforms), but regulates only the former, and only those that fall within the jurisdiction of Ukraine. This means that the most popular online platforms among Ukrainians such as Telegram, Facebook, Instagram, YouTube, Netflix, TikTok, etc. are not obliged to comply with the UML.

According to the UML,[359] VSPs are obliged to: comply with the requirements on media ownership transparency;[360] foresee in their terms of service prohibitions against disseminating information that violates the requirements of the UML (including during armed aggression and post-conflict time[361])[362] as well as legislation on copyright and related rights; publish their terms of service and familiarise users with them; and provide in their

[356] Opryshko D., "Report on Ukraine" *in* Swiss Institute of Comparative Law (ed.), *Comparative Study on Blocking, Filtering and Take-Down of Illegal Internet Content*, Lausanne, 2015; Opryshko D., *Follow-up to the Comparative Study on "Blocking, Filtering and Take-Down of Illegal Internet Content, Report on Ukraine*, 2019.
[357] Law of Ukraine on the media" No. 2849-IX, 13 December 2022.
[358] Such platforms may include Telegram, Facebook, X, etc.
[359] The obligations in the law are oriented by the according provisions in the AVMSD, specifically Articles 28b and further articles.
[360] Articles 25, 26, and 120 of the UML. These requirements aim to prohibit any connections with the aggressor state, whether through ownership or financing. For more information, see Opryshko D., "Regulation of Media in the Context of Armed Aggression" *in* Batura O., Holznagel B. and Kalbhenn J.C.(eds.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*, Nomos, 2024, pp. 254-257.
[361] The special provisions, foreseen in Chapter IX of the UML, apply only to an aggressor state officially recognised as such by the Parliament of Ukraine. The application of these provisions is limited in time – until this status is revoked and for five years after such a revocation. As of August 2025, Ukraine applied the status of "aggressor state" only to Russia (in 2015), after it illegally occupied part of the Ukrainian territory.
[362] Such restrictions include 14 general categories (Article 36 of the UML), information that may harm the physical, mental or moral development of children (Article 42 of the UML) and four special types of content, whose dissemination is prohibited, while the provisions of the Chapter IX are in force (Article 119 of the UML).

terms of service a procedure for exercising the right to reply to or refute inaccurate information. They are also obliged to: ensure verification of a user's age before allowing access to information that may harm the physical, mental or moral development of children; ensure the possibility of using a parental control system to protect children from such information; implement transparent and comprehensible mechanisms for filing complaints, particularly those related to the dissemination of illegal content, for their effective consideration, for informing complainants about the results of such complaint reviews, as well as to ensure a transparent, simple, and effective mechanism for appealing against actions taken by providers of VSPs regarding the consideration of such user complaints; implement effective media literacy measures and tools, and raise user awareness of such measures, etc.[363] If a VSP violates its obligations under the UML, the National Television and Radio Broadcasting Council of Ukraine (National Council) may apply relevant fines.[364]

The users of VSPs are empowered to appeal against unlawful decisions, actions, and any inaction on the part of VSPs to the National Council and/or to a court,[365] while providers of VSPs have the right to establish a co-regulatory body.[366]

Ukrainian legislation only provides for "soft" mechanisms for interacting with online platforms that are not under the jurisdiction of Ukraine. In this regard, the UML empowers the media regulator and other state bodies to take measures to establish cooperation with such platforms, including by concluding relevant agreements or memoranda.[367] Although negotiations with some companies, such as Meta and Google, have been underway for about a year, no memoranda or agreements have yet been concluded.[368] By the end of 2024, there were still no effective legal mechanisms in place to have an effect on online platforms

[363] Part 1 of Article 23 of the UML.

[364] Article 114, and Part 19 of Article 116 of the UML. For significant violations, VSP providers are subject to a fine of between 5 and 25 minimum wages as of the date of the violation. When determining the fine, the National Council must consider the technology used to provide the service, the territory of service provision, the audience reach, and other circumstances that affect the level of public danger posed by the violation that has been committed. As of August 2025, the approximate sum of the fine would amount to between EUR 870 and EUR 4 350.

[365] Part 3 of Article 23 of the UML.

[366] According to the UML, co-regulatory bodies are established by the representatives of the media industry and together with the National Council are entitled to develop codes (rules) for the creation and dissemination of certain information, criteria for prohibited information (*inter alia*, hate speech, discrimination, incitement to terrorism, child pornography), criteria for classifying persons as subjects in the field of online media, criteria for classifying advertisements as harmful, etc. This mechanism envisages that subjects in the media sphere voluntarily undertake to comply with the respective codes (rules), while the National Council recognises that these requirements are sufficient to ensure public interest (part 2 Article 36, paragraphs 23, 24, 26, 51 of Part 1, Part 2 Article 90, Article 92 of the UML).

[367] Part 15 of Article 2, paragraphs 13 and 14 of Part 1 of Article 90, paragraphs 3, 11 and 13 of Part 1 of Article 91, Part 3 of Article 99, Part 5 of Article 124 of the UML.

[368] Opryshko D., "Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), 2025, p.13; "National Television and Radio Broadcasting Council of Ukraine, platform regulation and who funds media registration companies: National Council meets with American Chamber of Commerce", Press release, 15 April 2025, available at: https://webportal.nrada.gov.ua/regulyuvannya-platform-ta-hto-finansuye-kompaniyi-yaki-reyestruyut-media-natsionalna-rada-provela-zustrich-z-amerykanskoyu-torgovelnoyu-palatoyu/.

that are not under Ukrainian jurisdiction but operating within Ukraine.[369] As of August 2025, no significant changes had taken place in this regard.

This poses a challenge for Ukraine, particularly given the systemic, large-scale and targeted information attacks Russia has conducted against the country and its people. The situation becomes more alarming due to the constant increase in information and news consumption through social platforms.[370]

In this context, it should be noted that Telegram became the most popular online platform in Ukraine following the start of the Russian full-scale invasion in February 2022. This is because it made it very easy to access information, contained channels that notified people of the direction of drones and rockets launched towards Ukraine, etc. In addition, many government officials, including those at the highest level, created their own channels on the Telegram platform to communicate with Ukrainian citizens.[371] Telegram maintained its status as the leading online platform in Ukraine at least until the end of 2024.[372]

At the same time, this online platform is being actively used in the course of Russian hostile information operations, for cyber attacks, to spread phishing messages and malicious software, to establish users' geolocation and correct missile strikes,[373] to recruit citizens (including minors) to commit violations against Ukraine (such as blowing up the military command bodies responsible for implementing Ukrainian legislation on military duty, military service and mobilisation training; and damaging or destroying the property (such as cars) of military personnel, etc.).[374]

This became the impetus for the development of several draft. laws, aimed at regulating online platforms, including the draft law on amending certain laws of Ukraine on the regulation of activity of shared access to information platforms through which mass information is disseminated.[375]

According to the explanatory note, the purpose of this draft law is to provide state authorities with the tools to effectively respond to national security threats originating from online platforms, particularly Telegram.[376]

---

[369] Opryshko D., "Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), 2025.
[370] Ibid, p. 6.
[371] Horbyk R., Dutsyk D. and Shalaysky S., "The Effectiveness of Countering Russian Disinformation in Ukraine in the Context of a Full-Scale War. Analytical report", NGO "Ukrainian Institute of Media and Communication", 2023, pp. 7 and 50.
[372] InMind, "Ukrainian media, attitude and trust in 2024", November 2024, pp. 4 and 28.
[373] The National Security and Defence Council of Ukraine decided to restrict the use of Telegram in state authorities, military formations, and critical infrastructure facilities, see here.
[374] Kharkiv Regional Military Administration, "Cyber police warn: recruitment of teenagers to commit sabotage has increased on the Internet", 19 February 2025; Ministry of Internal Affairs of Ukraine, "Enemy recruiting teenagers to commit sabotage: cyber police warn of dangers on the Internet", 12 March 2025; Patoka M., "The SSU revealed how many minors were arrested for collaborating with the Russian Federation", 30 June 2025.
[375] Law On Amending Certain Laws of Ukraine on the Regulation of Activity of Shared Access to Information Platforms Through Which Mass Information is Disseminated, No. 11115, 25 March 2024 (draft law).
[376] Explanatory note to the draft Law of Ukraine On Amending Certain Laws of Ukraine on Regulation of Activity of Shared Access to Information Platforms Through Which Mass Information Is Disseminated, No. 11115 of 25 March 2024, available here.

The authors of the draft attempted to incorporate elements of the DSA's approach to regulating online platforms into Ukrainian legislation. For instance, they suggested that platforms not falling under the jurisdiction of Ukraine or an EU member state should be required to appoint an authorised representative in Ukraine to facilitate communication with the National Council, other state authorities, and local self-government bodies.

However, the proposed amendments to the draft do not provide sufficient legal certainty. They fail to clarify why online platforms that disseminate mass information should be treated differently to other online platforms, given that both types of platforms provide the possibility of saving and spreading user information to an unlimited audience. The draft does not clarify whether the proposed provisions only regulate platforms targeting their activities at Ukraine and its population. Furthermore, it is unclear on what basis platforms falling under the jurisdiction of an EU member state(s) should communicate with the Ukrainian authorities regarding notifications, demands, decisions, applications, letters, or other documents, sent to them by the relevant Ukranian bodies.

This draft qualifies providers of online platforms through which mass information is disseminated as subjects in the media sphere, but unlike the EMFA and the DSA, it does not clarify the issue of editorial responsibility in this regard.[377] It also does not foresee the inclusion of court mechanisms in cases relating to restrictions on access to content whose dissemination violates the requirements of the UML, based on requests from the media regulator, etc.

As of August 2025, the draft was still under consideration by the Parliamentary Committee on Humanitarian and Information Policy and has not yet been submitted to the *Verkhovna Rada* (Ukranian Parliament) for the first reading.

Meanwhile, in September 2024, the National Cybersecurity Coordination Centre (NCCC) under the National Security and Defence Council of Ukraine (NSDC) recommended prohibiting the installation and use of Telegram on the official devices of employees of state authorities, military personnel, employees of the security and defence sector, as well as enterprises that are operators of critical infrastructure (with the exception of persons for whom the use of this messenger is part of their official duties).[378] These recommendations were followed by a number of public authorities, state universities and other entities.

In connection with this recommendation, the National Council also announced the introduction of a special regime of access to Telegram. The media regulator's employees were prohibited from using Telegram on their work devices (for the protection of classified information). At the same time, a separate network segment (separated from the internal

[377] According to the EMFA, providers of very large VSPs could be qualified as both a VSP provider, a VLOP provider and a media service provider when they exercise editorial control over a section or sections of their services (Recital 11). Exemptions from the liability foreseen in the DSA should not apply, *inter alia*, in relation to the information that has been developed under the editorial responsibility of the provider of the intermediary service itself (Recital 18).

[378] National Security and Defence Council, "The NCCC Has Decided to Restrict the Use of Telegram in Government Agencies, Military Formations, and Critical Infrastructure Facilities", Press release, 20 September 2024.

network of the National Council but connected to the external Internet) has been created to analyse the activities of media on this online platform.[379]

3.4.2. Specific rules regarding disinformation

A number of Ukraine's strategic documents define combatting disinformation and special information operations, as well as increasing the population's media literacy level, as goals.[380]

In 2022, the Russian full-scale invasion led to the introduction of martial law[381] on the whole territory of Ukraine and the imposition of restrictions on the right to freedom of expression[382] together with the derogation by Ukraine from its obligations under Article 19 of the International Covenant on Civil and Political Rights (ICCPR)[383] and Article 10 of the ECHR.[384] Although no censorship was officially introduced, Ukrainian legislation was amended and foresaw new rules, aimed at combatting Russian information influence.

This included, for example, the introduction of criminal liability for the justification, recognition as legitimate, or denial of the armed aggression by the Russian Federation against Ukraine, or the glorification of its participants;[385] the temporary blockings of on-demand audiovisual media services and services of audiovisual service providers of the aggressor state on the territory of Ukraine;[386] and the introduction of obligations for VSPs

[379] National Television and Radio Broadcasting Council of Ukraine, "The National Council Has Introduced a Special Procedure for Accessing Telegram", Press release, 9 October 2024,

[380] They were defined as priorities of state policy in the information sphere of Ukraine, *inter alia*, in the Doctrine of Information Security of Ukraine (2017-2021), and as strategic goals in the Information Security Strategy (2021), with the planned implementation period until 2025. In addition, see the Strategy of the Ministry of Culture and Information Policy of Ukraine on the Development of Media Literacy for the period until 2026, available here.

[381] Martial law is a special legal regime imposed in Ukraine or certain territories in the event of armed aggression or the threat of aggression, or any threat to the independence of the state of Ukraine and its territorial integrity; it provides for the granting of powers to appropriate state authorities, the Armed Forces Command, military administrations and local governments necessary to avert the threat, to repel the armed aggressor and to ensure national security, to eliminate the threat to the independence of the state and the territorial integrity of Ukraine, as well as to provide for the temporary threat-related restriction of constitutional rights and freedoms of persons and citizens, and the rights and legitimate interests of legal entities, specifying the duration of such restrictions (Article 1 of the Law of Ukraine On the Legal Regime of Martial Law of 12 May 2015, No. 389-VIII).

[382] Opryshko D., "Freedom of Expression during Military Conflict" in ORF (ed.), *Public Value Texte 25 – Why Independence Matters*, ORF, Wien, 2022, pp. 45-53, 46.

[383] International Covenant on Civil and Political Rights (adopted 16 December 1966) 999 UNTS 171.

[384] Opryshko D., "Monitoring Media Pluralism in the Digital Era: Application of the Media Pluralism Monitor in the European Union, Albania, Montenegro, the Republic of North Macedonia, Serbia and Turkey in the Year 2022. Preliminary Study to the Implementation of the Media Pluralism Monitor: Ukraine", EUI, RSC, Centre for Media Pluralism and Media Freedom, 2023, pp. 7-8.

[385] See Law of Ukraine On amendments to certain legislative acts of Ukraine regarding the strengthening of criminal liability for the production and distribution of prohibited information products of 3 March 2022.

[386] Article 123 of the UML. As of August 2025, 49 services have been included in the list of on-demand audiovisual media services and services of providers of audiovisual services of the aggressor state. The relevant list is available here.

to include temporary prohibitions on disseminating four special types of content in their terms of service.[387]

The latter include (1) information that portrays the armed aggression against Ukraine as an internal conflict, civil conflict, or civil war; (2) non-reliable materials about armed aggression and acts of the aggressor state (occupying state), its officials, persons and organisations controlled by the aggressor state (occupying state), if their dissemination leads to incitement of hostility or hatred.[388] This is explained by the fact that Russia systematically uses disinformation narratives, such as "internal conflict/civil conflict/civil war" or "conduct of a special operation on denazification/desatanisation" to justify its illegal actions, as well as to divide and weaken Ukrainian society.[389]

Moreover, to reduce the amplifying effect of disinformation narratives supported by Russian artists and musicians,[390] the Law of Ukraine prohibits the dissemination of (3) programmes and materials (except for information and analytical content), in which one of the participants is an individual included in the list of persons who present a threat to national security[391] and (4) music phonograms, videograms and music clips performed by singers who are citizens of the aggressor state (with some exceptions) and who have not condemned Russian aggression against Ukraine and are therefore included in the relevant list.[392]

3.4.3. Application in the case of foreign interference by disinformation in times of war

The provisions of the UML that regulate VSPs under Ukrainian jurisdiction have not yet been applied. This is because such platforms only began to register in Ukraine in 2025. As of August 2025, there are two VSPs that fall under Ukrainian jurisdiction.[393]

It should be noted that the UML establishes different regulatory approaches for the online platforms and media that have registered their accounts on these platforms as online media. The latter shall comply with requirements of Ukrainian legislation, including rules on ownership transparency, and may be held liable for violating the UML. Countering disinformation, misinformation and propaganda on anonymous accounts and channels

[387] While the provisions of Chapter IX of the UML are in force, as mentioned above, the special provisions foreseen in this chapter apply only to an aggressor state officially recognised as such by the Parliament of Ukraine. The application of the provisions is limited in time – until the status of aggressor state is revoked and for five years after such a revocation.
[388] Paragraphs 7 and 8 of part 4 of Article 112, paragraphs. 1 and 2 of part 1 of Article 119 of the UML.
[389] Opryshko D., "Regulation of Media in the Context of Armed Aggression" in Batura O., Holznagel B. and Kalbhenn J.C. (eds.), *Disinformation in Europe. Challenges, Legal Instruments & Policy Recommendations*. Nomos, 2024, pp. 251-252.
[390] Ibid., pp. 252-254; Batura O. and Opryshko D., "*Kunstfreiheit und Propaganda aus Sicht des Völkerrechts*", in Crückeberg J. et al. (eds.), *Handbuch Kulturpolitik*, Springer VS, Wiesbaden, 2023.
[391] This list includes, *inter alia*, famous theatre and film actors, directors, producers, composers, singers, TV presenters, etc., who publicly support Russia's war against Ukraine. The list is available here.
[392] Paragraphs 3 and 4 of part 1 of Article 119 of the UML.
[393] The list of subjects in the media sphere of 1 August 2025, pp. 6208, 6455, available here.

remains much more problematic. Such channels frequently have huge audiences (up to one third of Ukraine's population in absolute numbers)[394] and, therefore, strong influence on society. However, Ukraine cannot apply its legislation to them due to a lack of jurisdiction with regard to the aforementioned online platforms.

The state's lack of effective mechanisms to influence foreign online platforms in order to protect its national interests has led to widespread blocking of websites and online platforms. Such blocking is mainly implemented on the basis of the Ukrainian law on sanctions and during the Russian full-scale invasion of Ukraine; it is also implemented pursuant to orders from the National Centre for Operational and Technical Management of Telecommunication Networks (NCU). Both mechanisms are constantly criticised by human rights lawyers, experts, and industry associations, *inter alia*, due to their lack of transparency and foreseeability.[395]

The first instances of blocking web resources under the Law of Ukraine on Sanctions began in 2017 and concerned, among others, such Russian online platforms as VKontakte, Odnoklassniki, the Mail.ru email service, and the Yandex search engine and Internet portal.[396] The legal ground for such blocking became paragraph 25 of part 1 of Article 4 of the Law of Ukraine On Sanctions, namely "other sanctions that comply with the principles of their application as established by this law". This manner of blocking web resources has been criticised for not complying with the principles of "lawfulness" and "foreseeability" as required by Article 10(2) of the ECHR. However, in terms of restricting the dissemination of harmful content, experts consider such blocking to be a proportionate action for the protection of national security, personal data, copyright and related rights, and for countering pirated content, and not a violation of the right to the freedom of expression.[397]

Another previously mentioned mechanism for blocking web resources, including blocking access to digital network (IP) addresses and autonomous systems (AS), which is applied during the martial law in Ukraine, includes orders to block web resources issued by the NCU.[398] Non-compliance with the NCU orders may result in the exclusion of electronic

[394] Rodak K., "Trukha: true colours revealed. Who really stands behind the largest network of anonymous Telegram channels in Ukraine and how much it costs", 5 September 2023; Sklyarevs'ka G., NGL.media: "Trukha is owned by Volodymyr Lytvyn and earns hundreds of thousands of dollars a month from advertising"; Opryshko D., "Media Ownership Transparency as a Shield against Foreign Interference: the Ukrainian Experience", EMFA Observatory, EUI, 26 March 2025.

[395] Opryshko D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), 2025, pp. 15-17.

[396] Decree of the President of Ukraine On the Decision of the National Security and Defence Council of Ukraine of 28 April 2017 On the Application of Personal Special Economic and Other Restrictive Measures (Sanctions), 15 May 2017 No. 133, available here. Decisions on the blocking of online resources pursuant to the Law of Ukraine on Sanctions are adopted by the National Security and Defence Council of Ukraine and enacted by Presidential Decree (paragraphs 2 and 3 of Article 5 of the Law of Ukraine On Sanctions).

[397] Opryshko D., "Monitoring Media Pluralism the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), 2025, pp. 15, 20.

[398] Part 8, Article 32 of the Law of Ukraine On Electronic Communications.

communications networks and service providers from the relevant registry, consequently suspending their activities for one year.[399]

Restricting access to IP addresses and ASs significantly impacts not only those disseminating harmful content, but also other resources that are not subject to restrictions.[400] This results in the impossibility of accessing a large number of web resources situated alongside hostile propaganda resources on a single digital address, which are not related to the Russian war against Ukraine or Russian propaganda. Experts emphasise that the practice of AS blocking is unique and not applied anywhere else in the world.[401] The blocking of web resources based on the NCU's orders lacks sufficient transparency and predictability and does not guarantee protection against arbitrary blocking,[402] and has, therefore, been criticised for not complying with European standards in the field of freedom of expression.

[399] See, for example, the Decision of the National Commission for State Regulation in the Spheres of Electronic Communications, Radio Frequency Spectrum and Provision of Postal Services (NKEK) of 30 March 2022, No. 26 On Exclusion of the Limited Liability Company NETASSIST from the Register of Operators, Providers of Telecommunications with amendments made by the decision of the NKEK of 1 June 2022, No. 59.
[400] Belovolchenko A., "It is impossible to Reliably Block Something on the Internet. How Russian Resources are Blocked in Ukraine and Why it Affects Legal Sites" DOU.ua, 13 January 2023.
[401] Opryshko D., "Monitoring Media Pluralism in the European Union: Preliminary Study to the Implementation of the Media Pluralism Monitor 2025 in Ukraine", EUI, RSC, Research Project Report, Centre for Media Pluralism and Media Freedom (CMPF), 2025, pp. 16-17.
[402] Ibid., p. 17.

4. Countering terrorist content

4.1. Enforcement at EU level

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

The dissemination of terrorist content has expanded over the years in the online sphere, as terrorists spread their messages extensively using platforms that host third-party uploaded content.[403] This has already been acknowledged in the AVMSD, which emphasises the importance of shielding the general public from incitement to terrorism.[404] Accordingly, the AVMSD imposes an obligation on member states to ensure by appropriate means that services by audiovisual media service providers under their jurisdiction do not contain any public provocation to commit a terrorist offence;[405] equally, video-sharing platform (VSP) providers have to take appropriate measures to avoid such content on their platforms.[406] These measures include mechanisms for content reporting and flagging, age verification systems, parental control tools, and transparent content moderation procedures.[407]

The accessibility of terrorist content online has played a key role in radicalising individuals.[408] Thus, the Terrorist Content Online Regulation (TCOR)[409] has been a direct response to the limitations of voluntary arrangements under the EU Internet Forum,[410] which is a multi-stakeholder initiative launched by the European Commission in December 2015. While the EU Internet Forum has received positive responses with regard to improving cooperation among the industry, Europol and national authorities, only a limited number of hosting service providers are engaged in the EU Internet Forum. Also, the "scale and pace of progress" among hosting providers was not considered sufficient to address the

[403] Europol, "European Union Terrorism Situation and Trend Report 2023", Publications Office of the European Union, Luxembourg, 2023 and, Europol, "European Union Terrorism Situation and Trend Report 2022", Publications Office of the European Union, Luxembourg, 2022.
[404] See Recital 18 of the AVMSD explaining the introduction of a specific provision concerning the prohibition of dissemination of terrorist content in Article 6 of the AVMSD.
[405] AVMSD, op. cit.
[406] Ibid., Article 28b(1)(c).
[407] Ibid., Article 28b(3).
[408] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on preventing the dissemination of terrorist content online" COM(2018) 640 final, 2018 (Explanatory Memorandum); European Commission, "Report from the Commission to the European Parliament and the Council on the implementation of Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online" COM(2024) 64 final, 2024.
[409] Report on the implementation of Regulation (EU) 2021/784, op. cit., 17 May 2021. For an overview, see Voigt, P., Eschborn, E. and Bastians, H., *Weitreichende neue Pflichten für Host-Provider, Kurzanalyse der Verordnung zur Bekämpfung der Verbreitung terroristischer Online-Inhalte*, MMR 727, 2022.
[410] European Commission, "EU Internet Forum: Bringing together Governments, Europol and Technology Companies to Counter Terrorist Content and Hate Speech Online", Press release, 3 December 2015.

problem of the accessibility of terrorist content online.[411] Consensus regarding the need for stronger EU action against terrorist content online resulted in a 2018 Commission Recommendation.[412] This built upon the 2017 Commission Communication on tackling illegal content online[413] and the activities of the EU Internet Forum which outlined key measures including notice-and-action mechanisms. The suggested measures were later incorporated into the TCOR which provides harmonised rules on removing terrorist content and became applicable in June 2022.[414]

The TCOR relies on the definitions of terrorist offences as set out in Directive 2017/541 on combatting terrorism[415] and further defines to which material the definition of terrorist content online shall be applicable.[416] In this vein, the broad concept of terrorist content encompasses not only content that incites the commission of a terrorist act, but also materials related to recruitment, training or the provision of instruction, or those that encourage participation in a terrorist group or pose a risk of encouraging an individual to conduct a terrorist act.[417] Directive 2017/541 includes a list of intentional acts, defined as offences under national law, which legally constitute terrorist offences, e.g. attacks upon a person's life which may cause death, kidnapping or hostage-taking, etc. In Article 21, it also includes a number of measures to be taken against online content constituting a public provocation to commit a terrorist offence.

Applying to all hosting providers offering services in the EU,[418] Article 3 of the TCOR introduces "removal orders" and empowers the competent authorities to issue such orders requiring hosting providers to remove terrorist content or to disable access to terrorist content in all EU member states. The removal orders may be issued in the form of an administrative or judicial decision depending on the authority designated as competent. The TCOR seeks to increase the speed of reaction and ensure the blocking or removal of content at its source. Accordingly, the order to remove or disable access to terrorist content

[411] European Commission, "addressing the dissemination of terrorist content online", op. cit. ali here
[412] European Commission, Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online, OJ L 63/50, 2018.
[413] European Commission, "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, Tackling Illegal Content Online, Towards an Enhanced Responsibility of Online Platforms", COM(2017) 555 final, 2017.
[414] On the Proposal for a TCOR see Cole M.D., Etteldorf C. and Ullrich C., *Cross-Border Dissemination of Online Content*, Bd. 81 *Schriftenreihe Medienforschung*, Nomos, Baden-Baden, 2021, pp. 149 ff. For further details regarding the final TCOR see Albus, V.H., "Eyes Shut, Fingers Crossed: the EU's Governance of Terrorist Content Online under Regulation 2021/784" in Gsenger, R. and Sekwenz, M-T. (eds.), *Digital Decade: How the EU Shapes Digitalisation Research*, Nomos, Baden-Baden, 2025, pp. 209 ff.
[415] Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA, OJ L 88/6, 31 March 2017.
[416] Article 3 of Directive 2017/541 on combatting terrorism sets out a number of offences which should be defined as terrorist offences under national law when committed with the aim of seriously intimidating a population, unduly compelling a government or an international organisation to perform or abstain from performing any act, or seriously destabilising or destroying the fundamental political, constitutional, economic or social structures of a country or an international organisation.
[417] TCOR, op. cit., Article 2(7).
[418] Ibid., Article 1(2).

has to be executed as soon as possible and in any event within one hour of receipt of the removal order.[419]

To ensure swift processing of orders, a template set out in Annex I to the TCOR shall be used by the competent authorities and Article 15 of the TCOR requires hosting service providers to designate or establish a contact point for the receipt of these orders by electronic means. Hosting providers that do not have their main establishment in the EU shall designate a legal representative in the EU for the purpose of the receipt of, compliance with and enforcement of removal orders and decisions. Before issuing a removal order, the competent authorities should exchange information, coordinate and cooperate with each other and, where appropriate, with Europol to avoid duplication of effort and possible interferences with investigations.[420] Referrals, as a mechanism to alert hosting service providers to potential terrorist content for the provider's voluntary review against its terms and conditions,[421] are not regulated under the TCOR. However, they remain an effective and swift means of increasing hosting service providers' awareness of terrorist content available through their services and enabling them to take voluntary action.[422]

As regards cross-border removal orders within the EU, the TCOR introduces a new procedure, requiring, *inter alia*, the issuing member state to submit a copy of the order to the competent authority[423] of the hosting provider's main establishment with the aim of allowing the receiving authority to scrutinise the removal order; although the receiving authority should be able to assume that the removal order issued in another member state is lawful, it has the possibility to scrutinise itself whether the order has been issued according to the provisions of the TCOR and does not otherwise violate standards guaranteed by the Charter of Fundamental Rights of the European Union (CFREU).[424]

Further, the TCOR foresees additional due diligence obligations for hosting providers to apply so-called "specific measures" when they have been identified as a provider that has previously been exposed to terrorist content.[425] The specific measures include the identification and preventive removal of terrorist content;[426] however, there is no obligation for hosting providers to use automated tools to identify or remove content – which would also contravene the prohibition against imposing general monitoring

[419] TCOR, op. cit., Article 3(3).
[420] Ibid., Article 14. As regards the avoidance of duplication, member states are encouraged to use the dedicated tools developed by Europol, such as the EU Internet Rerferral Unit's *Plateforme Européenne de Retraits des Contenus illégaux sur Internet* (PERCI) (See Europol, "PERCI TCO Regulation Presentation" (7 November 2022)). PERCI aims at centralising, coordinating and facilitating the transmission of removal orders and referrals; it helps member states' competent authorities to prepare corresponding removal orders or referrals, and to transmit these to dedicated points of contact.
[421] TCOR, see Recital 40.
[422] Ibid.
[423] For a list of national competent authorities and contact points see the dedicated website of the European Commission.
[424] TCOR, Article 4.
[425] Ibid., Article 5(4).
[426] TCOR, Article 5.

obligations on intermediaries as laid down in Article 8 of the DSA and previously the eCommerce Directive.[427]

The European Commission is tasked with closely monitoring the implementation of the TCOR.[428] In order to increase awareness of the actions taking place under the TCOR, a hosting service provider that took action against the dissemination of terrorist content or has been required to take action under the TCOR must make publicly available transparency reports on those actions.[429] Since the TCOR does not introduce civil liability for hosted content, it relies on a system of sanctions. Accordingly, Article 18 of the TCOR obliges member states to lay down penalty rules; the systematic or persistent failure to comply with the takedown obligations is subject to financial penalties of up to 4% of the host provider's annual global turnover.[430]

Despite its very limited scope of application, both in the type of content concerned and in the fact that the addresses are only those of hosting service providers, the report on the implementation of the TCOR concludes that it has had a positive impact in limiting the dissemination of terrorist content online.[431] However, looking at details in that report, the European Commission only received information about 349 removal orders issued by the competent authorities[432] of six member states (Spain, Romania, France, Germany, Czechia and Austria) from June 2022 to 31 December 2023.[433] The deployment of the technical tool PERCI developed by Europol on 3 July 2023 as a new communication channel addressing illegal content online resulted in an increase in referrals with more than 14 000 referrals processed by the end of 2023.[434] The transmission of takedown requests – now in the form of removal orders – remained a challenge where hosting service providers are based in third countries and failed to appoint a legal representative in the EU.[435]

In parallel to the TCOR and the monitoring of its implementation, the European Commission continued its work with the member states, Europol and the industry acting on a voluntary basis, including in the framework of the EU Internet Forum. For instance, under the EU Crisis Protocol, a voluntary mechanism that allows EU member states and online platforms to respond rapidly and in a coordinated manner to the spread of terrorist content online in the event of a terrorist attack, a tabletop exercise was performed in 2024.[436] Further, Europol has been involved in developing a "database of hashes" of known terrorist

[427] European Union, 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 (eCommerce Directive).
[428] TCOR, op. cit., Article 21.
[429] Ibid., Article 7(2).
[430] Ibid., Article 18(3).
[431] European Commission, Report on the implementation of Regulation (EU) 2021/784, op. cit. op. cit.
[432] For a list of national competent authorities and contact points see the dedicated website of the European Commission.
[433] European Commission, Report on the implementation of Regulation (EU) 2021/784, op. cit.
[434] Ibid.
[435] Ibid.
[436] Europol, "Tabletop Exercise Hosted by Europol to Disrupt Terrorist Content Online", Press release, 7 March 2024.

content to allow content identified as harmful to be tagged electronically with the aim of preventing its reappearance.[437]

It must be noted that the DSA applies without prejudice to the rules laid down by the TCOR, meaning that the liability regime of the TCOR has priority over the related provisions of the DSA in terms of, for instance, the execution of a removal order.[438] Pursuant to Articles 16(5) and 16(6) of the DSA**,** VLOPSEs have to notify without undue delay individuals or entities of content moderation decisions, providing further information on possible redress, meaning that they will also have to inform the individuals or entities concerned when they take action upon a referral or a removal order.

It must be noted that the DSA covers a wider range of services than the TCOR, but VLOPSEs are of particular interest in terms of measures targeting the spread of terrorist content. Due to the systemic risks inherent in VLOPSEs, the providers of these services have to carry out, *inter alia*, a risk assessment in relation to the dissemination of illegal content, including terrorist content, and the anticipated negative effects on human rights, according to the DSA. The risks associated with the spread of illegal content must be diligently noticed, analysed and addressed.[439] The exposure to terrorist content varies significantly between VLOPSEs due to their very diverse nature.

Once a systemic risk of dissemination and exposure to terrorist content is identified, mitigation measures require the VLOPSE in question to coordinate and communicate with diverse actors. Any measures that VLOPSEs adopt towards terrorist content should be reasonable and effective in mitigating the specific systemic risks identified.[440]

In contrast, under the TCOR, a hosting service provider is only required to implement "specific measures" including measures mitigating its level of exposure to terrorist content, once its exposure to terrorist content has been formally established by the competent authority for the provider. The competent authority's decision must be based on objective factors such as the receipt of at least two removal orders within one year.[441] This form of mitigation is thus reactive, whereas the DSA requires VLOPSEs to become proactive when they have to conduct a preventive risk assessment. While codes of conduct are available for other areas of risk, the TCOR itself already provides for mitigation measures with reference to referrals, the tool of removal orders and "specific measures" once a hosting provider has been exposed to terrorist content.[442]

In addition, Article 18 of the DSA requires hosting providers that become aware of information giving rise to a suspicion that a criminal offence involving a threat to the life or safety of a person has taken place, is taking place or is likely to take place, to promptly inform law enforcement or judicial authorities and provide relevant information. While the

[437] European Commission, "A Counter-Terrorism Agenda for the EU and a Stronger Mandate for Europol: Questions and Answers", Press release, 9 December 2020.
[438] DSA, op. cit., Article 2(4)(c).
[439] Ibid., Recitals 53 and 55.
[440] Ibid., Recital 86.
[441] TCOR, Article 5(4).
[442] Ibid., Articles 3-5; Recital 40.

offences are not specified, Recital 56 of the DSA notes that this should cover offences under Directive 2017/541 on combatting terrorism, such as incitement to terrorism.

Using its investigatory and enforcement powers under the DSA, the European Commission has already opened formal proceedings against VLOPs, such as X, for an inadequate assessment of the risk of dissemination of terrorist content (in particular in the context of the Hamas terrorist attacks against Israel)[443] stemming from the design and functioning of the service.[444] In the future, due to the transparency and reporting obligations under both the TCOR and the DSA, more insights will be possible into the exposure of intermediaries to terrorist content and the measures taken to prevent the spread of such content.

4.2. The example of Germany

Dr Sandra Schmitz-Berndt, Research Associate, Institute of European Media Law (EMR)

4.2.1. National legal framework concerning platforms

Following the adoption of the DSA, platform regulation in Germany underwent several changes including the passing of the *Digitale-Dienste-Gesetz* (Digital Services Law – DDG)[445] implementing the DSA. It applies to all digital services in the sense of Article 1(1)(b) of the DSA unless otherwise specified within the DDG. The DDG also resembles the DSA in its structure and unifies pre-existing intermediary regulation in one single legal act, including the relevant elements of the national transposition of the AVMSD and the liability exemptions for intermediaries. It complements the DSA in allocating competencies, such as designating the *Bundeskriminalamt* (Federal Police Office – BKA)[446] as the competent authority for the notification of suspicions of criminal offences under Article 18 of the DSA.[447] The competent authority for the supervision of providers of intermediary services and enforcement of the DSA is the B*undesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen* (Federal Network Agency for Electricity, Gas, Telecommunications, Post and Railway – BNetzA) serving as the Digital Service Coordinator (DSC) for Germany. The DSC acts with full independence in carrying out the tasks and exercising the powers assigned to it. The DDG also lays down the rules on penalties applicable to DSA infringements.

[443] European Commission, "Commission Opens Formal Proceedings against X under the Digital Services Act", Press release, 18 December 2023.
[444] Commission Decision initiating proceedings pursuant to Article 66(1) of Regualtion (EU) 2022/2065, COM(2023) 9137 final, 2023.
[445] *Bundesgesetzblatt* (BGBl) (The Federal Law Gazette), 2024 I, No. 149.
[446] *Bundeskriminalamt* (Federal Police Office - BKA).
[447] DDG, paragraph 13.

Although the national legal framework changed significantly with the adoption of the DSA, it is worth examining the pre-DSA legal landscape, particularly the *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act – NetzDG),[448] which attracted considerable attention[449] both within and beyond Germany and is regarded as a policy that inspired the DSA and, before that, the TCOR.[450] The NetzDG provided a list of criminal offences that constituted "unlawful content" and imposed upon social network providers an obligation to maintain an effective and transparent procedure for handling complaints about such unlawful content.[451] Under the procedure, a provider was required to remove manifestly unlawful content, in general, within 24 hours.[452] The provider was also required to maintain an effective and transparent procedure that allowed both the complainant and the user whose content was reported to request a review of the decision to remove the content. In addition, social networks falling within the scope of application of the NetzDG were obligated to report any "unlawful content" amounting to one of the offences listed in paragraph 3a of the NetzDG to the BKA, which had established a central reporting office, the *Zentrale Meldestelle für strafbare Inhalte im Internet* (Central Reporting Office for Criminal Content on the Internet – ZMI BKA). These offences included the dissemination of propaganda material of terrorist organisations, the use of symbols of terrorist organisations and the formation of terrorist organisations. Furthermore, a biannual reporting obligation was introduced in order to gain insight into the management of complaints; this was complemented by a reporting obligation on mitigation efforts relating to "criminally punishable activities", a flagging mechanism, the implementation of content moderation and details about decision-making.[453] Information on moderation practices also covered the professional qualifications of human content moderators, including their linguistic expertise, which is a requirement now also reflected in the DSA. With the entry into force of the DSA, major parts of the NetzDG were repealed in 2024 and only the obligation to designate an authorised recipient for the service of documents remains,[454] while the obligations upon providers are now integrated into the DDG as stated above.

As regards the liability of platform providers for third-party content, there is a significant body of case law by German courts including the *Bundesgerichtshof* (BGH),[455] mainly addressing the applicability of the liability exemption of the previously applicable German implementation of Article 14 of the eCommerce Directive (which has now been replaced by Article 6 of the DSA), the scope of takedown and stay down obligations as well

[448] Network Enforcement Act (*Netzwerkdurchsetzungsgesetz* – NetzDG) of 1 September 2017, BGBl. I, p. 3352. English translation available here. For an overview of the initial version of the NetzDG, see Schmitz, S. and Berndt, C., *The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?*, 2018.

[449] For the controversial debate see Schulz, W., "Regulating Intermediaries to Protect Privacy Online – the Case of the German NetzDG" in Schulz, W. , Kettemann, M.C., and Heldt, A.P. (eds.), *Probleme und Potenziale des NetzDG – ein Reader mit fünf HBI-Expertisen*, *Arbeitspapiere des Hans-Bredow-Instituts*, 48, 2019, pp. 13 ff.

[450] Holznagel, D., "*Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act—Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierung, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen*", *Computer und Recht,* 2021, pp. 123-132; Kahl, J. and Liepert, S., "Digital Services Act: *Was sich gegenüber dem NetzDG ändert*", heise online, 9 December 2022.

[451] NetzDG, paragraphs 1; 3.

[452] Ibid., paragraph 1 II.

[453] Ibid., paragraph 2.

[454] Ibid., paragraph 5.

[455] The *Bundesgerichtshof* (BGH) is the supreme civil and criminal law court in Germany.

as the German concept of *Störerhaftung* (literally: 'liability as a disturber'). The latter is a strict liability regime derived from property law which entitles proprietors to request that any interference having detrimental effects on their property be removed and enjoined in the future even if the interference is not directly caused by the person addressed by the proprietor.[456] Once a platform provider is made aware of an infringement, not only must it grant injunctive relief to the injured party also ensure preventive measures.

EU legal acts are increasingly replacing and amending national legislation in the digital sphere, meaning that beside the DSA with its liability regime and rules on systemic risk mitigation, *inter alia*, the GDPR, DMA or the TCOR provide directly applicable rules in relation to platforms providing services in Germany as in all other member states.

4.2.2. Specific rules regarding terrorist content

The *Strafgesetzbuch* (German Criminal Code – StGB) sets out a variety of criminal offences related to terrorism including: the dissemination of terrorist propaganda material,[457] the use of symbols of terrorist organisations,[458] support for terrorist organisations,[459] public incitement to commit criminal offences including acts of terrorism,[460] and the approval of acts of terrorism.[461/462]

The enforcement of national criminal law, however, often reaches its limits when content is disseminated online: these limits may be of a factual nature (e.g. the actual perpetrator cannot be identified), of a jurisdictional nature (e.g. lack of territorial nexus), or of a practical nature (e.g. the challenge of enforcing national criminal law against foreign actors).[463] Challenges also arise where a particular behaviour such as Holocaust denial constitutes a criminal offence under German law,[464] but is perceived as legal in other states. To ensure that terrorist content is taken down expeditiously on large social media platforms, the NetzDG referred to Holocaust denial in a category of its own and introduced

[456] Paragraph 1004 of the *Bürgerliches Gesetzbuch* (BGB); see BGH, *Internet-Versteigerung* (11 March 2004) I ZR 304/01 36; BGH, *Internet-Versteigerung II* (19 April 2007) case No. I ZR 35/04; BGH, *Internet-Versteigerung III* (30 April 2008) I ZR 73/05. Under this strict liability regime, a person is held (indirectly) liable for enabling or facilitating someone else's illegal activity, even though the person did not commit the illegal act him/herself; to establish liability it is sufficient that the person played a role in causing or allowing the violation. Accordingly, in the aforementioned case law, the provider of an auction website could be held liable for contributing to a violation for example by providing the platform that enabled illegal listings, while the provider knew or should have known about the illegal activity and failed to act despite having the technical ability to stop or prevent the infringement.

[457] *Strafgesetzbuch* (German Criminal code – StGB), paragraph 86.

[458] Ibid., paragraph 86a.

[459] Ibid, paragraphs 129a-b.

[460] Ibid., paragraph 111.

[461] Ibid., paragraph 140.

[462] These offences had all been included in the list of criminal content materials that required expeditious removal under the NetzDG.

[463] See Ukrow J., "Introduction and Overview" in Cappello M. (ed), *Media Law Enforcement without Frontiers, IRIS Special*, European Audiovisual Observatory, Strasbourg, 2018, pp. 3 ff.

[464] StGB, under paragraph 130, see Heger M., "Paragraph 130 StGB" in Lackner K. and Kühl K. (eds.), Strafgesetzbuch, C.H. Beck, München, 31st ed. 2025, paragraphs 8 ff.

the outlined takedown regime (see above 4.2.1.). The TCOR follows an approach similar to the one contained in the NetzDG targeting primarily hosting service providers offering services within the EU.

With the adoption of the TCOR and the DSA, new layers of compliance have been introduced and the takedown and staydown obligations now fall directly under applicable harmonised EU law. However, some implementing measures were required under national law, mainly as regards the competent authorities and enforcement at national level.

Germany designated the BKA as responsible for issuing removal requests pursuant to Article 3 of the TCOR as well as scrutinising removal orders addressed to German hosting service providers from authorities in other EU member states. In addition, the BNetzA serves as the competent authority to oversee technical safeguards and issue penalties. Accordingly, the BNetzA supervises the implementation of specific measures such as content moderation pursuant to Article 5 of the TCOR for hosting service providers established in Germany and also takes the decision under Article 5(4) TCOR as to whether a hosting service provider can be regarded as being exposed to terrorist content online.[465] The BNetzA is also responsible for all proceedings concerning administrative fines under the TCOR. The BKA is the contact point under Article 12(2) of the TCOR and competent to receive notifications regarding content involving an imminent threat to life under Article 14(5) of the TCOR. Both the BKA and the BNetzA have to publish information and transparency reports, *inter alia*, under Article 8 of the TCOR.[466] To enforce the above-mentioned orders pursuant to Article 3(1) and Article 5(6) of the TCOR, a coercive fine of up to EUR 5 million may be imposed in accordance with the *Verwaltungsvollstreckungsgesetz* (Administrative Enforcement Act – VwVG).[467] In addition, detailed penalty provisions are contained in paragraph 6 *Terroristische-Online-Inhalte-Bekämpfungsgesetz* (Law to combat terrorist content online – TerrOIBG)[468] with administrative fines of up to EUR 5 million for individuals and up to 4% of the global annual turnover for legal entities.

Besides these regulatory frameworks, the ZMI BKA, which was established as the central reporting hub for the notification of suspicions of criminal offences under the NetzDG and continues this task for criminal offences with a threat to human life under the DSA, has also set up a voluntary cooperation with stakeholders to combat hate crimes. Although the focus is on hate crime, their scope is not limited to hate speech. Users can notify hate or extremist content to these stakeholders which will then assess the content and, if criminally relevant, forward the notification to the ZMI BKA for futher summary assessment and identification of the potential perpetrator. The status of a cooperation partner as a trusted flagger under the DSA does not impact the assessment; it simply means that notifications by trusted flaggers to hosting providers have to be treated as a priority by these providers. The cooperation partners are so far the state of Hesse,[469] a trust,[470] the

[465] This is regulated in the implementing act, the *Terroristische-Online-Inhalte-Bekämpfungsgesetz* (Law to combat terrorist content online - TerrOIBG), 29 April 2021.
[466] Ibid., Paragraph 4.
[467] Ibid., Paragraph 5.
[468] TCOR implementing act; TerrOIBG.
[469] Which operates the *Meldestelle HessenGegenHetze* for hate speech and extremist content.
[470] The trust *Jugendstiftung beim Demokratiezentrum Baden-Württemberg* operates REspect!, a reporting portal for hate speech.

media regulatory authorities of the German states (*Länder*) and public prosecutors.[471] These notification channels are intended to provide a low-threshold service in addition to filing a criminal complaint with a law enforcement authority. What renders the work of the ZMI BKA relevant in the context of terrorist content online is that the ZMI BKA must cooperate with the media regulatory authorities to initiate removal procedures for illegal content. These authorities are competent under the German *Jugendmedienschutz-Staatsvertrag* (Interstate treaty on the protection of minors in the media – JMStV) for the removal of a catalogue[472] of illegal content that also contains terrorist offences, including the depiction of cruel or otherwise inhuman acts of violence against people in a manner that glorifies or trivialises such violence.[473] The enforcement powers extend to fines and further coercive measures in administrative law.

The media regulatory authorities also have enforcement powers to combat criminally relevant content under the *German Medienstaatsvertrag* (Media State Treaty – MStV), which also applies to Internet intermediaries. The enforcement powers extend to access providers if the content provider or hosting provider does not comply with an initial order to remove the illegal content concerned. Notably, a media regulator has issued as *ultima ratio* a blocking order against major German access providers to block access to pornography platforms.[474]

4.2.3. Application following the Hamas terrorist attack in Israel in October 2023

In the wake of the terrorist attack by Hamas in Israel on 7 October 2023, Internet users became exposed to terrorist material on an unprecedented scale. During the attack, Hamas specifically leveraged Internet technologies by, *inter alia*, live-streaming their atrocities using mobile phones and bodycams on platforms such as Telegram and Facebook.[475] Content was also edited in real time and disseminated via social media platforms.[476] Subsequently, social media platforms have also been exposed to hateful narratives framed through hashtags such as #freepalestine. Unlike most other EU member states, regulatory

[471] For instance, the public prosecution office Göttingen as the central authority for combatting hate crime online in the state of Lower Saxony operates a notification tool on a dedicated website.
[472] See paragraph 4 of the JMStV; and Ukrow, J., "Paragraph 4 JMStV" in Cole, M.D., Oster, J. and Wagner, E.E. (eds.), *Medienstaatsvertrag, Jugendmedienschutz-Staatsvertrag (HK-MstV)*, C.F. Müller, Heidelberg, 104th supp. ed. September 2025.
[473] See paragraph 20 of the JMStV. Paragraph 5b of the JMStV also contains an obligation for VSP providers to implement a notification procedure for illegal content. The obligation has been criticised for being contrary to EU law due to its disregard for the fully harmonising effect of the DSA and has so far has not had any relevance in practice, see Liesching M., "Paragraph 5b JMStV" in Liesching M. (ed.), *BeckOK Jugendschutzrecht*, C.H. Beck, München, 5th ed. 2025, paragraph 2.
[474] See Schmitz-Berndt S., "Berlin Administrative Court Rejects Application for Interim Legal Protection of Porn Platforms against State Media Authority Blocking Order", *IRIS* 2025-6:1/18, European Audiovisual Observatory, 2025.
[475] Cortellessa E., "The Oct. 7 Massacre Revealed a New Hamas Social Media Strategy", *TIME*, 31 October 2023.
[476] Loucaides D., "How Telegram Became a Terrifying Weapon in the Israel-Hamas War", *WIRED*, 31 October 2023.

authorities in Germany responded quickly in actively using the TCOR. Reasons for the swift utilisation of the possibilities offered by the TCOR are, first of all, that Germany has a historical and legal sensitivity to antisemitism and terrorism; further, the authorities already had some experience with the centralised reporting hub ZMI BKA that had already fulfilled the same role under the NetzDG as it does now under Article 18 of the DSA, namely as the competent authority to receive notifications of suspicions of criminal offences. The example of the Hamas attack and its aftermath with a significant increase in illegal content, disinformation as well as hate speech on social media[477] serves to illustrate the TCOR's takedown regime in practice.

As outlined above, from June 2022 to 31 December 2023, a total of 349 removal orders based on the TCOR were issued by the competent authorities of six member states. The majority of these removal orders – notably 249 – had originated in Germany.[478] All of these orders were addressed to hosting providers outside of Germany and have been complied with. In contrast, only two removal orders had been issued by competent authorities in another member state against German hosting providers. As regards the issue of orders and the assessment of cross-border requests, the BKA may cooperate with the national media regulatory authorities of the German states. In that respect, the *Landesanstalt für Medien* from North Rhine-Westphalia as a representative of all media authorities is regularly involved.

By 21 November 2023 most of the orders concerned the October 2023 Hamas attack on Israel and were addressed to Telegram.[479] In fact, the BKA issued 153 removal orders between 7 October and 21 November 2023 targeting propaganda from Hamas and Palestinian Islamic Jihad against Telegram and X.[480] In sum, the number of removal orders does not seem to be very high, which is based on the fact that, prior to issuing a removal order, the BKA regularly uses the instrument of "referral" or removal request, which is a call for action to hosting providers to react voluntarily.

In 2023, the BKA transmitted 7 240 referrals, of which 5 762 resulted in the content concerned being removed or access disabled. Due to the non-binding nature of these referrals, there is no obligation to handle these within a certain time frame. However, the BKA will verify that content is removed or disabled after two working days.[481] This period fulfils the requirement of "expeditious" action in the liability exemption of Article 6(1) of the DSA applicable to hosting providers. If a hosting provider does not react within that time frame, the BKA, where necessary, will issue a removal order. Removal orders can also be issued directly without a request for voluntary removal. In fact, in response to the Hamas and Palestinian Islamic Jihad content in October 2023 mentioned above, the BKA had first

[477] *Bundesministerium des Inneren* (German Federal Ministry of the Interior), "*Wellen des Hasses stoppen*" (Stop waves of hatred), Press release, 13 February 2024.
[478] BKA, *Umsetzung der TCO-Verordnung im Bundeskriminalamt, Transparenzbericht für das Jahr 2023*, 2024.
[479] See *Deutscher Bundestag*, "*Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus*", 2023, BT-Drs. 20/9688.
[480] Removal orders were issued against X (10 orders), Telegram (143), see ibid.
[481] BNetzA, "Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act", 2024, p. 7.

sent referrals and subsequently issued removal orders as these referrals were not acted upon.

In 2023, the BNetzA classified the first German hosting service provider as being exposed to terrorist content and required the provider to take the necessary measures to ensure that said provider ceased to make terrorist content publicly available pursuant to Article 5 of the TCOR.[482] The classification was based on the fact that the provider concerned had received a large number of referral requests from the BKA and two removal orders.[483] The provider subsequently increased the technical and organisational measures in place to address the dissemination of terrorist content online.

The BNetzA and the BKA consider the measures of the hosting service provider concerned generally effective in reducing the spread of terrorist content online, with notable improvements during the reporting period 2024. An evaluation is ongoing regarding the provider's independent identification and response capabilities. A survey of hosting providers has identified a number of different measures that have been adopted: organisational measures (e.g. those related to terms of use), technical measures (e.g. automated detection of extremist emoji combinations, restricting user names, URLs and blocked accounts) and manual measures (e.g. content moderation teams, assessment of trends and circumvention tactics).[484] In 2023, a total of 15 766 items of content were removed by the hosting service provider identified as being exposed to terrorist content due to specific measures taken in accordance with Article 5 of the TCOR.[485] In 100 instances, users issued a complaint challenging the removal of their content leading to the content being restored in nine cases.[486]

In 2023, hosting service providers received 139 data access requests[487] from the competent authorities in connection with terrorist content or activities, compared to only four in 2024.[488] This highlights the need for a mechanism for swift removal alongside criminal investigations, especially given the rise in referral and removal requests. Notably, in 2024, the BKA issued 482 removal orders, achieving a compliance rate of 95.9%.[489] The BKA also reviewed 11 removal orders issued by other member states, none of which was contested, and transmitted 17 045 referrals to hosting service providers (87.4% of which led to content removal or disabling).[490]

---

[482] Ibid.
[483] Ibid., p. 8.
[484] BNetzA, "Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act", 2025, pp. 8 ff.
[485] BNetzA, "Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act", 2024, p. 8.
[486] Ibid.
[487] Ibid.
[488] BNetzA, "Transparency Report as per Article 8 of the Terrorist Content Online Regulation and Section 4 of the Act Addressing Terrorist Content Online and Monitoring Report as per Article 21(1) of the Regulation and Section 3 of the Act", 2025, p. 9.
[489] BKA, "Transparenzbericht 2024 zur Bekämpfung terroristischer Online-Inhalte veröffentlicht", Press release, 2025.
[490] Ibid., p. 1.

Beside the TCOR framework, the ZMI BKA relies on its voluntary cooperation mechanism with online notification portals for hate speech. From 7 October to 20 November 2023, the BKA received from that source, for example, a total of 139 notifications of criminal relevance as incitement to hatred or violence against parts of the population (paragraph 130 StGB) and that have a connection to the Middle East conflict.[491]

Content has also been notified by platform providers under Article 18 of the DSA to the BKA. From October 2023 to December 2023, only 16 notifications had been made, which is mainly due to the obligations only applying to designated VLOPSEs, whereas the provision only started to apply to other intermediaries from 17 February 2024 onwards. Out of 1 773 notifications in 2024, 1 244 were of criminal relevance, with only nine notifications concerning terrorism specifically.[492]

It is difficult to extract the precise number of removal orders, referral requests and other notifications as well as effective takedowns relating to the Hamas attack. In February 2024, the Minister for the Interior stated that the overall number of referral requests from 7 October to 2023 to 6 February 2024 concerning terrorist content in relation to the Hamas attack amounted to over 3 500.[493] 290 removal orders were issued as a result of that.[494]

In light of the figures cited above, these numbers are significant and indicate that the increase in terrorist content was accompanied by a surge in takedown measures. The swift response is mainly the result of the relevant infrastructure and institutional framework already being in place before the TCOR came into force, and the respective stakeholders' prior experience. The stringent standards incorporated in the now abrogated NetzDG may have also contributed to sensitising providers to respond swiftly to takedown requests.

4.3. The example of Türkiye

Dr Mehmet Bedii Kaya, Associate Professor of IT Law, Istanbul Bilgi University

4.3.1. National legal framework concerning platforms

The Republic of Türkiye is a member of the Council of Europe and the Organisation for Security and Co-operation in Europe, and is also a candidate country for the European Union. The country has a notably high level of Internet penetration in the population. According to the Turkish Statistical Institute, Internet usage rose from 27% in 2004 to

[491] See *Deutscher Bundestag*, "*Antwort der Bundesregierung auf die kleine Anfrage der Fraktion der CDU/CSU – Drucksache 20/9299 – Social-Media-Terrorismus*", 2023, BT-Drs. 20/9688, p. 5.
[492] Out of the criminally relevant content, 1 046 items related to CSAM materials. Material considered not criminally relevant mainly concerned suicide announcements, which are not a criminal offence but constitute a serious threat to life. See Bundesregierung, *Bericht der Bundesregierung gemäß § 13 Satz 2 des Digitale-Dienste-Gesetzes*, 27 August 2025.
[493] *Bundesministerium des Inneren*, "*Wellen des Hasses stoppen*", op. cit.
[494] Ibid.

approximately 97% by 2024, marking a 3.6-fold increase over two decades. Current usage patterns reveal that WhatsApp, Instagram, and YouTube are the most widely used social media platforms. Among these, YouTube dominates in terms of data consumption, accounting for 46.1% of total Internet traffic, followed by Instagram at 13% and Netflix at 5.9%.[495] These figures underscore a user behaviour trend heavily oriented toward video-based content, with social media platforms constituting a substantial share of overall Internet traffic in Türkiye.

The Constitution of the Republic of Türkiye enshrines key civil liberties, including freedom of expression, freedom of the press, and the protection of both the physical and mental integrity of individuals. While domestic legal frameworks frequently draw inspiration from European Union standards, Türkiye, as a result of being a non-member, tailors these norms to align with its national priorities and socio-political context. The Constitution does not contain any specific provisions regarding technology. However, notably, a significant amendment in 2010 introduced a provision for the protection of personal data. Section 3 of Article 20 of the Constitution explicitly recognises the right to the protection of personal data.

Türkiye has developed a comprehensive regulatory infrastructure aimed at preserving public order across both physical and digital domains. Over time, the scope and intensity of these regulatory measures have expanded, reflecting a trend toward increasingly stringent controls.

The principal legislative instrument governing Internet activities in Türkiye is Law No. 5651 *İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun* (the Law on the Regulation of Broadcasts via the Internet and the Prevention of Crimes Committed through Such Broadcasts – Internet Law).[496]

The Internet Law primarily governs three regulatory domains:[497]

1) the legal, criminal, and administrative responsibilities of key Internet actors, including content providers, hosting providers, Internet service providers (ISPs), public Internet providers, and social network providers;[498]
2) the procedures for restricting access in response to specific criminal offences, with particular emphasis on emergency interventions;
3) the implementation of Internet filtering mechanisms and surveillance practices.

[495] For all figures see *Bilgi Teknolojileri ve İletişim Kurumu* (Turkish Information and Communication Technologies Authority), "*Türkiye Elektronik Haberleşme Sektörü, Üç Auylik Pazar Verileri Raporu*" (Electronic Communications Sector, Quarterly Market Data Report), 2025, pp. 54-56.

[496] *5651 İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun*, OJ 23 May 2007/26530. For a full translation of the Turkish Internet Law see here.

[497] The provisions protecting personality rights have been annulled by the Turkish Constitutional Court. New rules to replace these provisions have not yet been enacted.

[498] For a comprehensive review of the Turkish Internet Law see Kaya, M.B., "The regulation of Internet intermediaries under Turkish law: Is there a delicate balance between rights and obligations?", *Computer Law & Security Review* 32, 2016, pp. 759 ff.

Since its initial adoption, the Internet Law has undergone several amendments, notably in 2014, 2020, and 2022, reflecting evolving policy priorities and technological developments. In addition to legislative reforms, judicial interpretations, especially rulings by the Turkish Constitutional Court concerning platforms such as Twitter and YouTube, have contributed significantly to the evolving understanding and application of the law.[499]

While the Internet Law initially served as the principal regulatory instrument for Internet governance in Türkiye, the legislative landscape has since evolved to grant authority to numerous institutions through their respective legal mandates. As a result, a wide array of public bodies now possesses the power to identify, remove, and block unlawful online content. This decentralisation has led to a fragmented legal and institutional framework. Despite the proliferation of supplementary legislative provisions addressing Internet-related issues, the Internet Law remains the foundational legislation governing online content and the responsibilities of digital intermediaries.

As previously stated, the Internet Law primarily governs specific categories of actors, including content providers, hosting providers, (ISPs), public Internet access providers, and social network providers. Among these, hosting providers occupy a central role. Pursuant to Article 2(1)(m) of the Internet Law, hosting providers are defined as "natural or legal persons offering systems that host services and content".

The regulatory provisions applicable to hosting providers encompass a wide spectrum of platforms with diverse functions, operational models, and technical architectures. These include traditional web hosting services, such as shared hosting, cloud-based hosting, virtual private servers (VPSs), dedicated servers, co-location services, and virtual private networks (VPNs), as well as platforms offering file, image, video, blog, and email hosting. The scope further extends to social media networks, search engines, online auction platforms, digital marketplaces, and other online platform providers.[500]

The Internet Law lacks sufficient scope to adequately regulate the diverse range of hosting providers, whose operational models can vary significantly. Notably, the Internet Law stipulates that hosting providers may be classified according to the nature of their services, and differentiated in terms of their rights and obligations, based on principles and procedures to be established through secondary legislation. This provision was incorporated into the Internet Law in 2014;[501] however, no such classification has been implemented to date in relevant secondary law. Consequently, a single legal rule currently applies to all online platforms.

Under Article 5 of the Internet Law, hosting providers are not responsible for monitoring the content they host or for determining whether any unlawful activity has occurred. Their liability is limited to removing illegal content upon notification, in accordance with the Internet Law's notice-and-takedown mechanism. They are obligated to promptly remove unlawful content from being publicly available.

---

[499] The Constitutional Court of the Republic of Türkiye, *Twitter Case*, Individual Application No. 2014/3986, 2 April 2014; *YouTube Case*, Individual Application No. 2014/4705, 29 May 2014; See also *Internet Law Case*, Decision Call No. 2014/87, Decision No. 2015/112, 8 December 2015.

[500] See, Işık A., İnternet Aktörleri ve Egemenliğin Değişen Boyutları, On İki Levha Publishing, 2023.

[501] Amendment through Law No. 6518, OJ 19 February 2014/28918.

The central issue requiring clarification is the scope of this removal obligation, specifically, whether it necessitates the permanent deletion of the content from servers, or whether restricting access for users within Türkiye (or traffic originating from Türkiye) would suffice to meet the legal requirement. This ambiguity represents one of the most contentious aspects of the Internet Law. Article 2 of this law defines content removal as "removing the content from the servers or from the hosted content, by content or hosting providers". Accordingly, if a provider employs technical measures such as geo-blocking or country-specific content restrictions, it may still be held liable under the Internet Law's provisions.

The Internet Law also prescribes a wide array of judicial and administrative sanctions for hosting providers that fail to comply with court orders or administrative directives, or that neglect to cooperate with relevant authorities.

Under the Internet Law, the only category of online platform explicitly defined in addition to hosting providers is that of social network provider.[502] This designation was introduced in 2022, with the legislative revision largely inspired by Germany's NetzDG.[503]

Article 2(1)(s) of the Internet Law defines social network providers as "natural or legal persons who enable users to create, view, or share textual, visual, audio, location-based, or similar data for the purpose of social interaction". Social network providers are considered a distinct subcategory of hosting providers. Importantly, the application of provisions specific to social network providers does not exempt them from the obligations and liabilities they bear as hosting providers under the Internet Law.

As per Additional Article 4 of the Internet Law, foreign social network providers receiving over one million daily visits from Türkiye are required to appoint at least one legal representative within the country. Both foreign and domestic providers exceeding this threshold must respond to notice-and-takedown requests within 48 hours, and any refusal must be accompanied by a reasoned explanation.

Additionally, as per Additional Article 4, these providers are obligated to submit biannual reports in Turkish, containing statistical and categorical data on the execution of content removal and blocking decisions. Failure to comply with these obligations may result in administrative fines, with penalties for foreign providers reaching up to one million Turkish liras.

The primary instrument used under the Internet Law to combat unlawful online content is the decision to block access and remove such content. The most essential method for addressing legal violations on the Internet is the removal of content deemed illegal by court orders or, under certain conditions, by administrative authorities. If the content is not removed, access to the specific URL hosting the unlawful material shall be blocked; if this is technically unfeasible, access to the entire website may be restricted.

---

[502] Amendment through Law No. 7253, OJ 31 July 2020/31202.

[503] For a comprehensive review of social media regulation see Kaya, M.B., and Akıncı, M.F., "Social Media Regulation" in Eroğlu, M., Finger, M. and Köksal, E. (eds.), *The Economics and Regulation of Digitalisation: The Case of Türkiye*, Routledge, Abingdon, 2024. See also above at Chapter 4.2.1f on the *NetzDG*.

The Internet Law outlines a general framework for addressing various forms of illegal content, including:

1) Article 8 – combatting specific criminal offences;
2) Article 8/A – enabling access restrictions in emergency situations.
3) The Information and Communication Technologies Authority (BTK) plays a central role in managing Türkiye's communications infrastructure and in executing access-blocking decisions under the Internet Law.

Article 8 of the Internet Law sets forth a specific procedure for imposing access restrictions on websites found to contain unlawful content.[504] This provision does not authorise such restrictions for all criminal offences; rather, it applies exclusively to an exhaustive list of specified crimes. In other words, access to a website cannot be blocked unless the offence falls within the scope of the enumerated crimes explicitly defined in the law. The offences covered under Article 8 include the following:

1) encouragement of suicide
2) sexual abuse of children
3) facilitating the use of drugs or stimulants
4) supplying substances that are dangerous to health
5) obscenity
6) prostitution
7) providing space and facilities for gambling
8) crimes encompassed in Law No. 5816 *Atatürk Aleyhine İşlenen Suçlar Hakkında Kanun* (Law concerning crimes committed to the detriment of Kemal Atatürk)
9) illegal betting
10) crimes regulated under Article 27(1) and (2) of Law No. 2937 *Devlet İstihbarat Hizmetleri ve Milli İstihbarat Teşkilatı Kanunu* (Law on state intelligence services and the national intelligence organisation).

Access-blocking decisions may be issued by a public prosecutor during the investigation phase, and by the court during the prosecution stage. It is important to note that terrorism and terrorism-related offences are not included among the crimes listed under Article 8 of the Internet Law.

In 2015, the Internet Law underwent reform, introducing a highly debated provision under Article 8/A.[505]

In matters concerning the protection of life and property, national security, public order, crime prevention, or public health, a judge may issue a decision to block access or remove online content. In urgent situations, this authority may also be exercised by the President of the Republic or relevant ministries. In such cases, the final decision to block access or remove content needs to be made by the President of the Information and Communication Technologies Authority (BTK).

[504] See also Keser L., "Reports on practical experiences from selected countries – Turkey" in Cappello M. (ed.), *Media Law Enforcement without Frontiers, IRIS Special*, European Audiovisual Observatory, Strasbourg, 2018, p. 92.
[505] See ibid., p. 93.

Under Article 8/A of the Internet Law, once a decision to remove content or block access for one of the reasons contained in the provision is issued, hosting providers and social network providers are required to implement the measure within four hours from the moment they are officially notified.

Although the intervention in the availability of Internet content is primarily grounded in judicial orders, access restrictions may also be imposed by a decision of the president or relevant ministers. According to Article 8/A, when such a decision is made, based on a request from the President of the Republic or the competent ministries, the President of BTK is required to submit the decision to the criminal court of peace for judicial approval within 24 hours. The judge is required to issue a ruling within 48 hours; otherwise, the decision is automatically nullified.

Administrative measures aimed at restricting access to Internet content have become wide practice in Türkiye. Notably, Article 8/A has evolved into a general legal basis for the regulation of online content. This provision has increasingly been employed as a broad blocking mechanism. Over time, it has served as the foundation for decisions to restrict access to various social media platforms, including X, Wattpad, TikTok, and Instagram.[506]

Under the Internet Law, access-blocking decisions are implemented by targeting specific elements of the infringing content, such as the publication, a section of a publication, or the URL address. However, if it is technically unfeasible to restrict access solely to the unlawful content or its related components, authorities may resort to blocking the entire website.

The widespread use of encrypted traffic by websites has rendered URL-based blocking virtually ineffective. As a result, if the service provider fails to remove the targeted content, access to the entire website is typically restricted. This approach has become a long-standing regulatory practice. Consequently, access to entire platforms such as Google Sites, YouTube, and Wikipedia has been blocked in the past. This method of blanket blocking has been the subject of several rulings by the European Court of Human Rights against Türkiye.[507]

Türkiye has adopted a strategy of controlling online content primarily through IP and DNS-based restriction methods. To support this approach, the country's Internet infrastructure has been significantly upgraded to prevent access to content deemed unlawful by competent authorities. A comprehensive and advanced deep packet inspection (DPI) system has been deployed across all access points nationwide. Nonetheless, the growing prevalence of encryption technologies, especially the widespread use of encrypted traffic, has diminished the effectiveness of such inspection systems. As a result of these technological limitations, Türkiye has been compelled to reassess its model of "Internet censorship". This shift has coincided with a major transformation in Internet governance,

[506] See also Michaelson R., "The Internet's Sewer: Why Turkey Blocked Its most Popular Social Site", *The Guardian*, 1 March 2023; "*Ekşi Sözlük'e 'milli güvenlik ve kamu düzeninin korunması' gerekçesiyle yine erişim engeli getirildi* (Access blocking order against Ekşi Sözlük for the reason of 'protecting national security and public order')", *BBC*, 14 December 2023.

[507] See *Ahmet Yildirim v. Turkey*, Application No. 3111/10 (ECtHR, 18 December 2012); *Cengiz and Others v. Turkey*, Application Nos. 48226/10 and 14027/11 (ECtHR, 1 December 2015).

driven by the rapid expansion of social media, which now plays a central role in both social and economic spheres.

The new regulatory approach of Türkiye aims to address content management on social media platforms at its origin. Rather than simply limiting access, the focus is on ensuring that unlawful or harmful content is completely removed directly from its source. In line with this shift, the revised legislation mandates that social media companies appoint a local representative to facilitate direct engagement with Turkish authorities. These platforms are also required to respond promptly to user requests, submit transparency reports detailing their content moderation activities, keep personal data within Turkish borders, enhance their capacity to combat criminal activity, and take proactive measures to protect minors and young users. The revised social media regulations, i.e. Additional Article 4 of the Internet Law as introduced in 2022, have established a unique accountability structure tailored to Türkiye's policy objectives. To ensure effective enforcement of these provisions, the Internet Law has been supplemented with new sanction mechanisms. Social media platforms that fail to meet their legal obligations may face penalties such as advertising bans, bandwidth reduction, shared civil liability for unlawful content, and substantial administrative fines.

4.3.2. Specific rules regarding terrorist content

Türkiye has long been engaged in efforts to counter terrorism, having experienced numerous terrorist attacks over the years. This struggle has been pursued through both operational measures and legal instruments. In response to the legal dimensions of terrorism, a dedicated piece of legislation entitled the *Terörle Mücadele Kanunu* (Anti-Terrorism Law), was enacted in 1991 to establish the necessary legal framework for addressing such threats.[508]

This legislation provides a comprehensive framework by defining terrorism, specifying the individuals responsible for terrorist acts, outlining offences committed with terrorist intent, characterising terrorist organisations, and establishing distinct procedures and penalties applicable to such crimes.

Under the Anti-Terrorism Law, terrorism is defined as follows:

> *Terrorism is any kind of act done by one or more persons belonging to an organisation with the aim of changing the characteristics of the Republic as specified in the Constitution, its political, legal, social, secular and economic system, damaging the indivisible unity of the State with its territory and nation, endangering the existence of the Turkish State and Republic, weakening or destroying or seizing the authority of the State, eliminating fundamental rights and freedoms, or damaging the internal and external security of the State, public order or general health by means of pressure, force and violence, terror, intimidation, oppression or threat.*

[508] Full translation of the Turkish Anti-Terrorism Law here.

Terrorism, as defined by the Anti-Terrorism Law, may be perpetrated by individuals or groups.

Offences classified as terrorist crimes are those perpetrated in connection with the activities of a terrorist organisation. When an act is designated as a terrorist offence, it becomes subject to aggravated penalties and distinct procedural rules under the applicable legal framework.

Since its enactment, this law has remained a focal point of legal and political debate, with critics contending that it imposes disproportionate restrictions on fundamental rights and freedoms. Over time, its scope and provisions have undergone significant amendments.

4.3.3. Application in view of blocking access to terrorist content

Given that digital technologies were not prevalent at the time of its adoption, the Anti-Terrorism Law understandably lacks explicit references to the Internet or related technological domains. Nonetheless, its foundational definitions have continued to inform and shape subsequent regulatory frameworks governing the digital environment.

Unlike Article 8 of the Internet Law, which permits access blocking and content removal only for certain crimes, Article 8/A of the Internet Law permits access blocking and content removal for any criminal offence or breach of public order. Notably, terrorism and terrorism-related offences may fall within the scope of Article 8/A of the Internet Law, as the broad concepts of national security, public order, and crime prevention grant significant discretionary authority over Internet regulation.

The BTK does not maintain statistical records regarding websites blocked on grounds of terrorism, nor does it disclose any comprehensive data to the public in this regard. Nevertheless, press statements issued at various times indicate that terrorism-related content has been subject to blocking measures pursuant to Article 8/A of the Internet Law.[509]

In this context it must be noted that addressing terrorism remains one of Türkiye's most urgent priorities, and the country is actively engaged in combatting terrorist content online. Although the Internet Law, Türkiye's primary legal framework for Internet regulation, does not explicitly mention terrorist content, enforcement efforts continue in this domain. Article 8/A of the law functions as a broad provision, allowing intervention and access blocking for a wide range of unlawful content.

Accordingly, one may argue that Article 8/A of the Internet Law serves as a catch-all provision for controlling any online content. Notably, this means that in practice the very

[509] See "*6 bin 500 habere engel 5 bin habere sansür!* (6 500 news items blocked, 5 000 removed!)", *Cumhuriyet*, 16 October 2023; Uludag A., "*AYM kararına rağmen engellenen içeriklerin sayısı artıyor* (Despite the decision of the Constitutional Court, the number of blocked content items is increasing)", *Deutsche Welle*, 4 August 2023.

short time frame of four hours for removal applies to all terrorist content from all platforms, including social media.

5. Countering defamatory, hateful and violence-inciting speech

5.1. Enforcement at EU level

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

Several factors, including a succession of economic and social crises, the COVID-19 pandemic, challenges concerning migration and increased digitalisation, contributed to a proliferation of speech online that is defamatory, hateful and incites violence.[510] The EU's recent regulatory approach to countering these types of speech is constantly evolving.

To facilitate a harmonised enforcement approach, similar to the field of terrorist content (see above Chapter 4.1), the EU prompted an alignment of what should be considered as criminal and, thus, illegal speech in its member states. For example, illegal hate speech is defined in a Framework Decision on combatting certain forms and expressions of racism and xenophobia by means of criminal law[511] as public incitement to violence or hatred on the basis of certain characteristics, including race, colour, religion, descent and national or ethnic origin.[512] While this Framework Decision on combatting racism and xenophobia covers only racist and xenophobic speech, the majority of member states have extended their national laws to sanction hate speech based on other grounds, such as sexual orientation, gender identity and disability. This approach is also reflected in the consolidated AVMSD which in Article 6 generally and Article 9(1)(c)(ii) for commercial communications refer to a broader list of grounds of prohibited discrimination that includes sex, racial or ethnic origin, nationality, religion or belief, disability, age or sexual orientation and, thus, resembles Article 21 of the Charter of Fundamental Rights of the European Union (CFREU), which is expressly referenced in Article 6(1).[513]

---

[510] See Faloppa F. et al., *Study on Preventing and Combating Hate Speech in Times of Crisis*, Council of Europe, CDADI, Strasbourg, November 2023.

[511] European Union, 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 328/55, 6 December 2008.

[512] The EU has also adopted several directives prohibiting discrimination based on a variety of grounds, such as race and ethnic origin. Due to the scope of this IRIS report, these directives are not addressed.

[513] Since the CFREU provisions should be interpreted in the same way as the ECHR, the ECtHR jurisprudence on Article 17 ECHR clarifies the minimum European human rights threshold for criminal hate speech. This was distilled in paragraph 11 of the Council of Europe, Committee of Ministers' Recommendation on Combating Hate Speech, CM/Rec/(2022)16, which includes: a. public incitement to commit genocide, violence or discrimination; b. racist, xenophobic, sexist and LGBTI-phobic threats; c. racist, xenophobic, sexist and LGBTI-phobic public insults under conditions such as those set out specifically for online insults in the Additional

With fragmentation of the material law on one side and a sharp rise in hate speech and hate crime in Europe on the other,[514] in 2021, the European Commission adopted a communication which emphasises the need for a Council decision extending the current list of "EU crimes" as foreseen by Article 83(1) TFEU[515] to include hate speech and hate crime.[516] However, since such an extension of the list has not yet been formally concluded, the European Parliament and the Council do not have any legal basis to adopt secondary legislation establishing minimum rules concerning the definition of hate speech-related criminal offences and related sanctions.[517] Irrespective of these limits, the Directive on combatting violence against women and domestic violence[518] criminalises hate speech against women alongside other forms of gender-based cyber violence on the basis that violence against women endangers the core EU value of equality between women and men while relying on Articles 82(2) and 83(1) TFEU as legal bases.

In the meantime, strategies have emerged under EU primary, secondary and soft law to counter hate speech by clarifying key elements of the conceptualisation of hate speech.[519] Work on combatting hate speech online has been reinforced by regarding such speech as contravening core EU values enshrined in Article 2 of the Treaty on European Union(TEU).[520]

Protocol to the Convention on Cybercrime concerning the criminalisation of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189); d. public denial, trivialisation and condoning of genocide, crimes against humanity or war crimes; and, e. intentional dissemination of material that contains such expressions of hate speech (listed in a-e above) including ideas based on racial superiority or hatred.

[514] For the latter, see the annual reports of the European Commission against Racism and Intolerance (ECRI) of 2019 and 2020: ECRI, "Annual Report of ECRI's Activities Covering the Period from 1 January to 31 December 2019", Strasbourg, March 2020 and ECRi, "Annual Report on ECRI's Activities Covering the Period from 1 January to 31 December 2020", Strasbourg, March 2021. See also the study commissioned by the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, "Hate speech and hate crime in the EU and the evaluation of online content regulation approaches", July 2020.

[515] The areas of crime listed in Article 83(1) of the TFEU are the following: 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.

[516] European Commission, Communication from the Commission to the European Parliament and to the Council, A more inclusive and protective Europe: Extending the list of EU crimes to hate speech and hate crime, COM(2021) 777 final, 2021.

[517] Pursuant to Article 83(1) of the TFEU, the European Parliament and the Council may, by means of directives adopted in accordance with the ordinary legislative procedure, establish minimum rules concerning the definition of criminal offences and sanctions in the areas of particularly serious crime with a cross-border dimension resulting from the nature or impact of such offences or from a special need to combat them on a common basis. On the status of proposals to extend the list of EU crimes to all forms of hate crime and hate speech see the dedicated legislative train schedule website of the European Parliament available at https://www.europarl.europa.eu/legislative-train/theme-protecting-our-democracy-upholding-our-values/file-hate-crimes-and-hate-speech.

[518] European Union, Directive (EU) 2024/1385 of the European Parliament and of the Council of 14 May 2024 on combatting violence against women and domestic violence, OJ L 2024/1385, 24 May 2024.

[519] See Nave E., and Lane L., "Countering Online Hate Speech: How Does Human Rights Due Diligence Impact Terms of Service", *Computer Law & Security Review* 51, 2023, 105884. In terms of policy measures, the European Commission established in 2016 a High-Level Group on combatting hate speech and hate crime which, *inter alia*, published guidance on cooperation between law enforcement authorities and civil society organisations, and serves to facilitate the exchange of best practice (see European Commission, *Informal Commission Expert Group "High Level Group on Combating Hate Speech and Hate Crime", Terms of Reference*, 2016).

[520] See European Commission, Joint Communication to the European Parliament and to the Council, "No Place for Hate: A Europe United Against Hatred", JOIN(2023) 51 final, 2023 (in response to online reactions to the Hamas attack on Israel on 7 October 2023).

With many initiatives and awareness campaigns targeting on- and offline hatred,[521] the focus of this chapter lies in the dissemination of such content on online platforms. Online platforms pose particular risks due to their algorithmic systems which amplify the spread of specific types of speech and, thus, may have serious and negative effects on potential victims.

Similarily, for defamatory speech, an effect as described for hate speech can be observed, because fast online dissemination and replication of such content continuously exposes victims of such speech to insults and potential further damages. However, unlike hate speech which can be restricted under Article 10 of the ECHR[522] or Article 11 of the CFREU, the situation with regard to defamatory statements is not as clear cut. Defamation is not always clearly illegal, in fact, offensive statements can still be protected under the ECHR and CFREU.[523] Whether or not defamatory statements have the level of illegality is determined by national law. The application of the standards generally requires an evaluation of factual accuracy, a consideration of context, public interest and intent. Similar challenges exist with regard to speech inciting violence.

Despite the challenges inherant in determining the nature of a given speech, the DSA introduces at the EU level a framework of layered responsibilities for online platforms. In particular, the DSA obliges VLOPSEs to address and mitigate the risks associated with the dissemination of illegal content under their specific obligations laid down in section 5 of Chapter III of the DSA. This additional obligation exists beside the general requirement imposed on all hosting service providers to have a notice-and-action system in place and to expeditiously remove illegal content that they are aware of. Further, they must be transparent about the functioning of their algorithms and recommender systems and address the risks of such systems acting as amplifiers for illegal content.

As regards hate speech, these obligations, including those for swift action, are grounded in the Code of Conduct on Countering Illegal Hate Speech Online,[524] which focuses on illegal hate speech as defined by the aforementioned Framework Decision. This code of conduct was at first a voluntary agreement between the European Commission and, originally, Facebook, Microsoft, Twitter and YouTube in 2016 and was later joined by further platform providers.[525] The Code of Conduct on Countering Illegal Hate Speech Online aimed to combat the spread of illegal hate speech online in compliance with EU and national laws by, *inter alia*, speeding up the review and removal of illegal hate speech, for most of the notifications giving a time frame of 24 hours for reaction, and promoting transparency and cooperation between platforms and EU authorities. On 20 January 2025, the code of conduct was revised and integrated into the co-regulatory architecture of the DSA as the Code of

[521] For an overview on work streams and resources at EU level see the dedicated Commission website "Combating Hate Speech and Hate Crime", available at https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/combating-hate-speech-and-hate-crime_en.

[522] Either for abuse of rights (Article 17 ECHR) or as destroying the fundamental values of the ECHR (and restrictions are deemed necessary under Article 10(2) ECHR). For a brief overview on the ECtHR case law on hate speech see ECtHR, Press Unit, "Factsheet – Hate Speech", 23 November 2023.

[523] *Handyside v. the United Kingdom*, Application No. 5493/72 (ECtHR, 7 December 1976).

[524] Code of Conduct on Countering Illegal Hate Speech Online, 30 June 2016.

[525] See the dedicated Commission website, available here.

Conduct on Countering Illegal Hate Speech Online +.[526] With a focus on the prevention and anticipation of threats, the Code of Conduct on Countering Illegal Hate Speech Online + seeks to enhance how platforms address illegal speech under EU and national laws and aims to support effective DSA enforcement. Adherence to the Code of Conduct on Countering Illegal Hate Speech Online + may serve as a valid risk mitigation measure for signatories that qualify as VLOPSEs.

Prior to its integration into the DSA, the European Commission initiated formal proceedings against X pursuant to Article 66(1) of the DSA (see above, Chapter 4.1). These proceedings alleged an infringement of Articles 34 and 35 of the DSA concerning risk assessment and mitigation, due to the inadequacy of the assessment of X's provider of the design and functioning of its "Freedom of Speech Not Freedom of Reach" system in the EU.[527] In particular, in 2023, X reduced its content moderation staff,[528] withdrew from the Code of Practice on Disinformation,[529] and dissolved its advisory group tasked with addressing hate speech.[530] Notably, the European Commission considered that

> *the regional and linguistic aspects of X's policies on 'Violent and Hateful Entities', 'Violent Speech', 'Hateful Content' and 'Sensitive Media', in the European Union, as well as the content moderation resources and other systems dedicated by TIUC and X Holdings Corp. to implement those policies appear inadequate to consistently and effectively mitigate the risk of disseminating illegal content.*[531]

A subsequent analysis of data submitted in November 2023 to the DSA Transparency Database revealed that X's content moderation is indeed limited when compared to other social media platforms.[532] In January 2025, the European Commission issued a retention order in the context of the ongoing investigation, requesting X to provide further information by way of technical investigatory measures relating to the platform's recommender system.[533] The European Commission requested access to certain commercial application programming interfaces (APIs), particularly the technical interfaces to the content on X that allow direct fact-finding on content moderation and virality of accounts. The duration of the investigation reflects the complexity of assessing systemic risks and

---

[526] Code of Conduct on Countering Illegal Hate Speech Online +, 20 January 2025. The Code takes the form of five commitments and two annexes. The commitments relate, *inter alia*, to a review of the majority of hate speech notices within 24 hours under Articles 16 and 22 of the DSA from so-called "monitoring reporters" with expertise in hate speech.

[527] Commission Decision of 18 December 2023 initiating proceedings pursuant to Article 66(1) of Regulation (EU) 2022/2065, COM(2023) 9137 final, paragraph 9, 2023.

[528] Reuters, "Twitter further Cuts Staff Overseeing Global Content Moderation, Bloomberg Reports", *Reuters*, 7 January 2023.

[529] See X post by Thierry Breton on "Twitter leaves EU voluntary Code of Practice against disinformation" of 26 May 2023.

[530] Associated Press, "Musk's Twitter Has Dissolved its Trust and Safety Council", *npr*, 12 December 2022.

[531] Ibid., paragraph 10. TIUC is the Twitter International Unlimited Company, the main establishment of the provider of X in the EU. X Holdings Corp. is the company controlling the group of legal entities to which TIUC belongs.

[532] Kaushal R. et al., "Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database", FAccT '24: Proceedings of the 2024 ACM Conference on Fairness, Accountability, and Transparency, pp. 1121-1132.

[533] European Commission, "Commission Addresses Additional Investigatory Measures to X in the ongoing Proceedings under the Digital Services Act", Press release, 17 January 2025.

their mitigation from the viewpoint of the supervisory authority. As of September 2025, X is still under investigation by the European Commission for its content moderation practices and transparency obligations. If the Commission determines that X has failed to comply with its obligations under the DSA, it may impose sanctions (see Chapter 2.2.2.2).

As regards the notice-and-action requirements established by the DSA, the challenges that have already arisen under the eCommerce Directive are likely to persist, such as the question of takedown and staydown for repeated infringements of the same type. Similar to the provisions under the eCommerce Directive, the DSA does not establish a general monitoring obligation for hosting service providers. However, parties that can claim to have had their rights infringed by content hosted by the providers have a strong interest in bringing an end to the illegal act and preventing the act of illegal content dissemination being continued or repeated. This is why they can resort to requesting an injunction with which they can seek to ensure that the respective content is taken down expeditiously by the providers and at the same time stays down and does not reappear.[534] Such a staydown requires an intervention by the hosting service provider, for instance by means of content moderation or filtering.[535]

While the question of specific filtering obligations has also been intensively debated in the field of copyright and related rights, particularly regarding Article 17 of the Copyright in the Digital Single Market Directive (CDSM),[536/537] the idea of takedown and staydown raises even more questions in the case of defamatory or libellous content: here, the unlawfulness of the content is not necessarily attributable to the use of certain words or phrases (for example, those regarded as insulting), but to the fact that the entirety of the statement made may be regarded as defamatory.[538] If the effective protection of an infringed party's rights was to be ensured, this would require that an injunction issued by a court covers not only the wording used in the content found to be unlawful, but also "information, the content of which, while essentially conveying the same message, is worded slightly differently, because of the words used or their combination" as it was put by the Court of Justice of the European Union (CJEU) in a case brought to it by an Austrian court.[539] The concept of "information with an equivalent meaning" was considered by the CJEU as permissible for an injunction issued by a national court as long as it would not require an independent assessment by the provider and an obligation to block that type of information

[534] See, with regards to intellectual property rights: C-324/09 *L'Oréal SA and Others v. eBay International and Others* (CJEU, 12 July 2011) ECLI:EU:C:2011:474; and C-70/10 *Scarlet Extended SA v. SABAM* (CJEU, 24 November 2011) ECLI:EU:C:2011:771.

[535] See Enarsson T., "Navigating Hate Speech and Content Moderation under the DSA: Insights from ECtHR case law", *Information & Communications Technology Law* 33(3), 2024, pp. 384-401.

[536] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/92 17 May 2019.

[537] See, for instance, Geiger C. and Jütte B.J., "Platform Liability under Article 17 of the Copyright in the Digital Single Market Directive, Automated Filtering and Fundamental Rights: An Impossible Match", *GRUR International* 70(6), 2021, pp. 517-543; Rauer N. and Bibi A., "*Grundrechtskonformität des Art. 17 DSM-RL – Ende gut alles gut?*", *Zeitschrift für Urheber- und Medienrecht*, 2022, pp. 585-672.

[538] *C-18/18 Glawischnig-Piesczek v Facebook* (CJEU, 3 October 2019) ECLI:EU:C:2019:821, paragraph 40.

[539] Ibid., paragraph 41.

overall.[540] This conclusion acknowledges that providers – due to the amount of information stored – typically use automated search tools and technologies in moderating and filtering content,[541] which therefore is not a check for every item posted in advance.

5.2. The example of Ireland

Dr Roderick Flynn, Associate Professor, Chair of Communications Studies, School of Communications, Dublin City University

5.2.1. National legal framework concerning platforms

The passage of the most recent (2018) iteration of the AVMSD and of the DSA in 2022 and the requirement to transpose or integrate both into Irish law, set in train an extensive set of additions to the Irish 2009 Broadcasting Act.[542] These additions relate to the regulation of hateful and violence-inciting speech online although they have relatively little to do with defamation which remains subject to the 2009 Defamation Act[543] .

One direct outcome of the AVMSD/DSA transposition and integration was the creation of a new media regulator *Coimisiún na Meán* (CnaM). CnaM superseded the Broadcasting Authority of Ireland (BAI), the regulatory remit of which was largely limited to radio and television broadcasters and on-demand services. The significant expansion of regulation to cover online content driven by the AVMSD and DSA demanded new regulatory structures given institutional expression by the establishment of CnaM on 15 March 2023. All functions previously vested in the BAI were transferred to CnaM along with the additional regulatory obligations stemming from the AVMSD and the DSA. The re-establishment saw the regulator relocate to new headquarters appropriate to the increased scale of the organisation, reflected in an increase in staff numbers from less than 50 to an anticipated 350 plus. In consequence, CnaM is the body responsible for ensuring that online platforms operate mechanisms to protect their users against harmful content, including hateful and violence-inciting speech, in an effective manner.

The inclusion of the AVMSD and DSA provisions in Irish law was largely achieved through two pieces of domestic legislation: the 2022 Online Safety and Media Regulation Act (OSMR)[544] and the 2024 Irish Digital Services Act.[545] The texts of both were added to the existing 2009 Broadcasting Act. As yet, no official consolidation of the legislation has been published although the Irish Law Society maintains an online version which includes all

[540] Ibid., paragraphs 46 ff.
[541] See Ibid., paragraph 46. For a comment on this see Rojszczak M., "Online Content Filtering in EU Law – A Coherent Framework or Jigsaw Puzzle?", *Computer Law & Security Review* 47, 2022, 105739.
[542] Broadcasting Act 2009.
[543] Defamation Act 2009.
[544] Online Safety and Media Regulation Act 2022.
[545] Digital Services Act 2024.

post 2009 additions to "the Principal Act" (i.e. the original text of the 2009 Broadcasting Act).[546]

Despite the passage of the OSMR, Ireland was slow to complete the transposition of some AVMSD elements (including those relating to video-sharing platforms (VSPs)) into domestic legislation. In February 2024, the CJEU imposed a fine of EUR 2 500 000 on Ireland for failing to fully transpose the AVMSD.[547] The CJEU found that while the OSMR contained provisions allowing for the (mandatory) adoption of codes aimed at VSPs, these codes had not been drawn up as of early 2024. This was finally addressed in October 2024, when CnaM published the Online Safety Code.[548] This is outlined in detail below but, in brief, the document spells out what constitutes harmful content and specifically cites incitement to violence or hatred directed against a group of persons or a member of a group based on any of the grounds referred to in Article 21 of the CFREU such as gender, political affiliation, disability, ethnic minority membership, religion and race. It also specifies the obligations of VSP service providers with regard to the content they host. It states that such platform providers "shall include, in the terms and conditions and related obligations of the service, restrictions that preclude users from:

- uploading or sharing restricted video content as defined in this Code, and
- uploading or sharing restricted indissociable user-generated content as defined in this Code."[549]

The Online Safety Code also states that where users have frequently infringed these terms and conditions, the platform provider shall suspend their account.[550] According to the code, CnaM has the task of identifying VSP services that are under Irish jurisdiction and designating these as such, which happened for the first time in December 2023 with most of the major VSP services active in Europe included.[551]

Reddit and Tumblr appealed their designation to the Irish High Court in 2024. Reddit argued that as a U.S. corporate body it should not be subject to the jurisdiction of the Irish state while Tumblr argued that the volume of video content on its platform was relatively low and thus did not meet the threshold for designating it as a VSP. In June 2024, the Irish High Court unambiguously dismissed both appeals stating that CnaM had designated both services in a proper manner.[552] In May 2025, however, CnaM revoked its

[546] See Law Reform Commission, Broadcasting Act 2009 (last updated 1 June 2025).
[547] Collins, S., "Ireland fined €2.5m by EU courts for delays to online safety law", *Irish Independent*, 29 February 2024.
[548] *Coimisiún na Meán*, Online Safety Code, October 2024.
[549] Ibid., section 12.1.
[550] Ibid., section 12.6.
[551] Given that a substantial number of platforms and tech companies have located their European headquarters in Ireland, in December 2023 CnaM designated 10 VSP services as subject to the – then still-to-be-published – Online Safety Code. These were: Facebook, Instagram, YouTube, Udemy, TikTok, LinkedIn, X/Twitter, Pinterest, Tumblr, and Reddit.
[552] O'Faolain, A., "High Court dismisses Reddit and Tumblr challenges over new online safety code", *Irish Times*, 20 June 2024.

designation of Reddit after the parent company of the latter relocated its European headquarters to the Netherlands.[553]

5.2.2. Specific rules regarding defamatory, hateful and violence-inciting speech

Defamation is only addressed in brief in this report because the Online Safety Code effectively makes no overt reference to libel or defamation. This is not to say that hateful or violence-inciting speech might not also constitute defamation. In practice, however, online defamation is legally treated as identical to defamation contained in print or broadcast content. As such, online defamation is governed by the provisions of the 2009 Defamation Act. It has been noted, however, that online defamation creates distinct challenges, not least in identifying the individual responsible for posting defamatory material via an online platform. In this regard attention must be drawn to provisions of the 2024 Defamation Bill which has been passed by the lower house of the Irish parliament and is currently (October 2025) going through committee stage scrutiny in the upper house of the parliament.[554] Noting the potential difficulty in identifying persons who post defamatory statements online, part 9, section 22 of the bill proposes to amend the 2009 Defamation Act to allow individuals to seek an order from the Circuit Court addressed to the relevant online platform ("information service provider") requiring that platform to disclose the identity of the individual who has posted defamatory material. Applicants for such disclosures of identity must demonstrate to the Circuit Court's satisfaction that defamation has occurred and, additionally, that a related defamation legal case is likely to succeed at trial.[555]

Concerning illegal and harmful content, under section 7(2)(d) of the 2009 Broadcasting Act (as amended), CnaM must endeavour to ensure that its regulatory arrangements "address programme material, user-generated content, and other content, which are harmful or illegal". Section 139K(3) of the Broadcasting Act specifically requires CnaM to create an online safety code applying to VSP service providers, as mentioned above.

Section 139A of the 2009 Broadcasting Act (as amended) defines the categories of harmful online content that the Online Safety Code deals with. Section 139A(2)(a) refers to schedule 3 of the legislation as outlining "offence-specific categories of online content". Section 4 of schedule 3 defines hateful and violence-inciting speech as "online content by which a person publishes or distributes written material, or a recording of visual images or

[553] *Coimisiún na Meán*, Revocation of Designation Notice, 22 May 2025.
[554] House of the Oireachtas, Defamation (Amendment) Bill 2024, Bill 67 of 2024.
[555] In passing, we would also note that in March 2022 four Irish members of parliament sponsored the "Responsibility of Social Media Platforms (Defamation Amendment) Bill" which would have allowed for judgments of defamation to be made against social media platforms on which defamatory utterances were made in situations where the social media platform in question was unable to produce the identity of the individual who made the utterances. As a private members' bill, however, the proposed legislation did not win the support of the government and did not progress through the Irish Parliament.

sounds, contrary to section 2(1) of the Prohibition of Incitement to Hatred Act 1989 (material, images or sounds which are threatening, abusive or insulting and are intended or, having regard to all the circumstances, are likely to stir up hatred)". According to section 5 of schedule 3, harmful content also includes broadcasts "contrary to section 3(1) of the Prohibition of Incitement to Hatred Act 1989 (threatening, abusive or insulting images or sounds whose broadcast is intended or, having regard to all the circumstances, is likely to stir up hatred)".

The reliance on the 1989 Prohibition of Incitement to Hatred Act[556] is potentially problematic because, as discussed below, the act is regarded as flawed. This act prohibits incitement to hatred against a group of persons on account of their "race, colour, nationality, religion, ethnic or national origins, membership of the travelling community or sexual orientation".

Although the 1989 Prohibition of Incitement to Hatred Act criminalises incitement to hatred it is primarily considered as a hate speech provision. Incitement includes publication, broadcast and preparation of materials and the application of the 1989 Act is not limited to offline behaviour as it extends to words used, behaviour or material displayed in "any place other than inside a private residence".[557]

However, the 1989 Prohibition of Incitement to Hatred Act is considered flawed: a 2016 Law Reform Commission report on Harmful Communications and Digital Safety noted that "the 1989 Act has been subject to significant criticism for its perceived inefficacy, illustrated by the limited number of prosecutions that have been taken under it".[558] Similarly, in its observations on Ireland, the UN Committee on the Elimination of Racial Discrimination has expressed concern that the 1989 Prohibition of Incitement to Hatred Act has been ineffective in combatting racist hate speech, particularly online racist hate speech.[559] Some academics have described the 1989 Prohibition of Incitement to Hatred Act as "manifestly not fit for the purpose of addressing hate crime", and in need of reform to take particular account of the context of cyber hate crime.[560]

To address these flaws, in 2021 the then government moved to replace the 1989 Prohibition of Incitement to Hatred Act with legislation providing for new and aggravated offences, including a new offence of incitement. The general scheme of a bill was published in April 2021 and this promised to make it a specific criminal offence to commit a hate crime based on the colour of a person's skin, sexual orientation or their gender, including gender expression or identity. Other new "protected characteristics" include the victim's race, nationality, religion, ethnic and national origin, and any disability.[561] A revised version

[556] Prohibition of Incitement to Hatred Act 1989.
[557] Ibid., section 2.(1)(b)(i).
[558] Law Reform Commission, "Harmful Communications and Digital Safety", Report LRC 116-2016, Dublin 2016.
[559] Committee on the Elimination of Racial Discrimination, "Concluding observations on the combined fifth to ninth reports of Ireland", UN, CERD/C/IRL/CO/5-9, Geneva 23 January 2020.
[560] Haynes, A. and Schweppes, J., "Lifecycle of a hate Crime: Country Report for Ireland", Irish Council for Civil Liberties, Dublin, 2017.
[561] Department of Justice, Home Affairs and Migration, "New Bill to tackle hate crime and hate speech includes clear provision to protect freedom of expression", Press release, 27 October 2022.

of the bill was published as the Criminal Justice (Incitement to Violence or Hatred and Hate Offences) Bill in October 2022.[562]

The new legislation was to criminalise any intentional or reckless communication or behaviour that was likely to incite violence or hatred against a person or persons because they were associated with any of the protected characteristics referred to above. The legislation also created new, aggravated forms of certain existing criminal offences, where those offences were motivated by hatred directed against a protected characteristic.

Despite some debate about the proposal, the new legislation was approved in 2023 by the lower house of parliament.[563] However, it stalled in the upper house after criticism by backbench parliamentarians and some senators. Eventually in October 2024 with the life of the parliament coming to a conclusion (there was a general election in November 2024), the then Minister for Justice decided that the most pragmatic course forward was to remove any reference in the legislation to incitement to violence or hatred (and to the EU Framework Decision on combatting racism and xenophobia).[564] In consequence then, the 1989 legislation remains the basis for defining hate speech and speech inciting violence.

5.2.3. The Online Safety Code in practice

In outlining the Online Safety Framework Ireland, CnaM stresses that, as the Irish media regulator, it cannot immediately remove content from the Internet. Rather, its role is to ensure that the online platforms (and broadcasters) which fall under its jurisdiction put in place measures to prevent illegal or harmful content being shown. Thus, primary responsibility for dealing with harmful content (including hate speech and speech inciting violence) rests with the platforms themselves. CnaM notes that platforms have a legal obligation to enforce their own rules relating to content and to provide mechanisms for users to report content which breaches those rules.

Given this, the role of CnaM is to intervene when these reporting mechanisms do not operate in the manner intended. CnaM advises users that, if they experience difficulties in submitting a report to a platform, or if they feel that a platform has not followed the correct procedures for handling a report, this should be reported to CnaM.

In the event that a user reports illegal content to a platform and they fail to receive a timely response and/or the content is not removed, CnaM advises users that they can report this. However, they note that their powers thereafter are limited: "Our Advice Centre will thank you for your report, give you advice and will record your concerns. We are not able to remove this content for you."

---

[562] Irish Council for Civil Liberties, "Better engagement with impacted communities paramount as hate crime and extreme hate speech legislation advances at the Oireachtas", Press release, 27 October 2022 (Dublin: ICCL).
[563] Public Interest Law Alliance, "New Bill to tackle hate crime and hate speech is currently before the Seanad", Press release, 17 May 2023.
[564] 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 328/55, 6 December 2008.

At best, CnaM may pass on the report to their Platform Supervision team "who will work to ensure that the platforms improve their systems". For more urgent content – direct online threats to the physical safety of an individual – CnaM advises users to contact the Irish police directly. Again, CnaM stresses that their role is limited to investigating systemic risks on platforms rather than specific incidents.

In this regard, although not directly related to Article 28b of the AVMSD, Article 34 of the DSA requires designated VLOPs and VLOSEs to identify, analyse and assess any "systemic risks … stemming from the design or functioning of their service and its related systems, including algorithmic systems, or from the use made of their services".

All 10 Irish-headquartered VLOPs and VLOSEs have submitted systemic risk assessments to the European Commission in line with Article 34 of the DSA.[565] These include sections relating to hate speech. Looking at the first assessments submitted, all 10 Irish-based platforms note the inherent risk that their platforms might be used for hate speech but assert that their internal mitigation measures mean that the actual risk is low. Against this, it is not in the interest of any platform to represent themselves as posing a significant risk with regard to illegal speech.

Given how recently the Online Safety Framework and related code have been put in place, it is perhaps too soon to offer an objective assessment of its efficacy. It is notable that in June 2025, CnaM felt compelled to issue a statutory Information Notice to the X platform on the grounds that X had failed to provide sufficient information to allow CnaM to determine whether X was taking sufficient measures to comply with the child protection element of the code.[566] X had previously, in December 2024, launched a legal challenge against the rules imposed on it under the Online Safety Code, arguing that these constituted "regulatory overreach"[567] and went further than Article 28b of the AVMSD required. This was rejected by the Irish High Court in July 2025 and in the same month X introduced new age assurance measures designed to address CnaM's child safety concerns.[568]

It is also worth noting the conclusions of research published by CnaM in September 2025 detailing the online experience of candidates in the Irish local and general elections of 2024.[569] Notably, although the June 2024 local elections preceded the publication of the Online Safety Code, the latter was in place before the November 2024 general election. The research found that 48% of local election candidates experienced either: offensive, abusive or hateful behaviour online; violent or intimidating behaviour online; or behaviour that involved impersonating a candidate online.[570] This increased to 59% of candidates in the November 2024 general election. The research added that 24% of local election candidates and 21% of general election candidates who "used social media and experienced relevant

[565] Tremau Digital Services Act Database. Accessed at: https://tremau.com/resources/dsa-database/, 31 October 2025. See also: DSA: Risk Assessment & Audit Database.
[566] *Coimisiún na Meán*, "Coimisiún na Meán issues statutory information notice to X", Press release, 17 June 2025.
[567] See Gallagher, F., "X Loses High Court Challenge Brought against Coimisiún na Meán Safety Code", *The Irish Times*, 29 July 2025.
[568] *X Internet UnLtd Company v. Coimisiún na Meán* [2025] IEHC 442
[569] *Coimisiún na Meán*, "On the digital campaign trail: Election candidates' online experiences in the 2024 elections", (Dublin: CnaM).
[570] Ibid.,Ibid., p. 5.

online behaviours received online threats to *kill or cause serious harm* to them during their election campaign"[571] (emphasis added).

Furthermore, 58% of local election candidates and 69% of general election candidates who experienced such behaviours did not report them to the relevant online platforms.[572] The reasons for not reporting included not knowing how to make a report, an inability to find the reporting function on a platform and the fact that the scale of hateful or violent content was too great to report all instances. However, by far the most common reason advanced (by 59% of local election candidates and 72% of general election candidates) was the belief that the report would not be dealt with effectively.[573] A "belief" may not constitute an absolutely compelling reason to conclude that the Irish Online Safety Framework is ineffective, but the results of this research can be seen as a cause for concern.

5.3. The example of Austria

Dr Clara Rauchegger, University of Innsbruck

5.3.1. National legal framework concerning platforms

5.3.1.1. The Austrian Communication Platforms Act

In 2020, the Austrian legislator adopted a bundle of legislative measures to combat online hate speech, defamation, cyber mobbing and other illegal behaviour on online platforms. The common goal for these measures was the fight against "hate on the Internet".[574] The *Hass im Netz-Bekämpfungsgesetz* (Hate on the Internet legislative package) entered into force in January 2021.

A central part of this bundle of legislative measures was the newly adopted *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen* (Communication Platforms Act – KoPl-G).[575] Following the example of the German *Netzwerkdurchsetzungsgesetz* (Network Enforcement Act – NetzDG),[576] it introduced a

[571] Ibid.,Ibid., p. 6.
[572] Ibid., p. 81.
[573] Ibid., p. 86.
[574] *Bundesgesetz, mit dem das Kommunikationsplattformen-Gesetz, das E-Commerce-Gesetz, das Mediengesetz, das Strafgesetzbuch, die Strafprozessordnung, das Einführungsgesetz zu den Strafgesetzen, das Allgemeine Bürgerliche Gesetzbuch und die Zivilprozessordnung geändert werden (Hass im Netz-Bekämpfungsgesetz)*, BGBl. I Nr. 151/2020.
[575] *Bundesgesetz über Maßnahmen zum Schutz der Nutzer auf Kommunikationsplattformen* (Kommunikationsplattformen-Gesetz – KoPl-G), BGBl. I Nr. 151/2020.
[576] Network Enforcement Act (*Netzwerkdurchsetzungsgesetz*, NetzDG) of 1 September 2017, BGBl. I, p. 3352. English translation available at:

number of obligations for large online platforms. They were required to provide a reporting system so that users could flag illegal content and to remove or block illegal content within 24 hours, for obviously illegal content, or seven days, if a detailed assessment was necessary to determine illegality.[577] The platforms were further required to publish transparency reports[578] and to appoint a responsible representative in Austria.[579]

5.3.1.2. The judgment of the CJEU invalidating the Communication Platforms Act

The KoPl-G was found to be incompatible with the eCommerce Directive[580] by the CJEU in its judgment in the case of *Google Ireland v. KommAustria*.[581] More specifically, the CJEU found a violation of the country of origin principle that is enshrined in the eCommerce Directive.

According to the country of origin principle, providers of information society services generally only have to comply with the national laws of their country of origin, i.e. the member state where they are established.[582] Countries of destination, i.e. member states where the services are offered, cannot impose their own legal rules on providers established in another member state.[583] The country of origin principle extends to the "coordinated field", which means all "requirements laid down in Member States' legal systems applicable to information society service providers or information society services, regardless of whether they are of a general nature or specifically designed for them".[584]

In 2000, when the eCommerce Directive was enacted, it seemed unrealistic for the EU to harmonise relevant legislation for information society services comprehensively.[585] At the same time, the EU wanted to support the development of information society services to foster innovation and economic growth and to "enhance the competitiveness of European industry".[586] In the absence of harmonised legislation in the relevant areas, the country of origin principle was meant to remove the "obstacles arising from divergences in legislation and from the legal uncertainty as to which national rules apply to such services".[587] The idea is that obstacles are removed by the rule that "information society services should in principle be subject to the law of the Member State in which the service

https://www.bmjv.de/SharedDocs/Gesetzgebungsverfahren/Dokumente/NetzDG_engl.pdf;jsessionid=798A2B22B939C8AEEA23B03619CC3544.2_cid289?__blob=publicationFile&v. For an overview of the initial version of the NetzDG see Schmitz, S. and Berndt, C., *The German Act on Improving Law Enforcement on Social Networks (NetzDG): A Blunt Sword?*, 2018.

[577] KoPl-G, paragraph 3.

[578] Ibid., paragraph 4.

[579] Ibid., paragraph 5.

[580] 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 July 2000.

[581] C-376/22 *Google Ireland v. KommAustria* (CJEU, 9 November 2023) ECLI:EU:C:2023:835.

[582] eCommerce Directive, Article 3(1).

[583] eCommerce Directive, Article 3(2).

[584] Definition of "coordinated field" in eCommerce Directive, Article 2(h).

[585] Raue B., "Case Note on CJEU, Google Ireland and Others, C-376/22", *Neue Juristische Wochenschrift*, 2024, pp. 201-205, 204.

[586] eCommerce Directive, Recital 2.

[587] Ibid., Recital 5.

provider is established".[588] They are "regulated solely in the Member State on whose territory the providers of those services are established",[589] with the eCommerce Directive permitting derogations from said principle under certain conditions.[590] In particular, the free movement of information society services can be restricted if this is necessary for reasons of public policy, public health, public security or consumer protection.[591] A central, substantive condition for this derogation is that the measure has to be "taken against a given information society service".[592] The central question in *Google Ireland v. KommAustria* concerned whether general and abstract measures applying generally to certain categories of information society services could be interpreted as measures "taken against a given information society service" and therefore justified as permissible derogations from the country of origin principle.[593] The CJEU in its judgment declared that they could not. The possibility of derogating from the country of origin principle does not extend to general and abstract measures such as those stipulated by the KoPl-G. The latter was therefore in the court's view adopted in violation of the eCommerce Directive.

The CJEU undertook a literal, systematic and teleological interpretation to reach this conclusion. Regarding the wording, the CJEU emphasised that the derogation provision referred to a "given information society service". The use of the singular and the adjective "given" indicated that the derogation did not extend to general and abstract measures aimed generally at a category of information society service.[594] In its systematic interpretation, the CJEU relied on the procedural conditions that member states have to comply with when seeking to derogate from the country of origin principle.[595] From a teleological standpoint, the CJEU stressed that the eCommerce Directive aimed to ensure the freedom of information society services, an objective pursued through the principles of home member state control and mutual recognition.[596] These principles would be called into question if member states were allowed to adopt general and abstract measures aimed at a category of information society services within the coordinated field.[597] Overall, the CJEU opted for an internal market-friendly interpretation of the county of origin principle.[598] It strengthened this principle and restricted the freedom of member states to adopt

[588] eCommerce Directive, op. cit., Recital 22.
[589] C-376/22 *Google Ireland v. KommAustria* (CJEU, 9 November 2023), paragraph 42. ECLI:EU:C:2023:835.
[590] eCommerce Directive, Article 3(4).
[591] Ibid., Article 3(4)(a)(i).
[592] Ibid., Article 3(4)(a)(ii).
[593] See C-376/22 *Google Ireland v. KommAustria*, op. cit., paragraph 25.
[594] Ibid, paragraph 27.
[595] eCommerce Directive, Article 3(4)(b); ibid [35-38].
[596] See C-376/22 *Google Ireland v. KommAustria*, op. cit., paragraphs 39-59.
[597] Ibid, paragraph 60.
[598] Knoke L., Krüger H. and Sachs, C., "*EuGH stärkt Herkunftslandprinzip: Zugleich Besprechung von EuGH Urt. v. 9.11.2023 – C-376/22, EuZW 2024, 137 – Google Ireland u.a.*", *European Journal of Business Law*, 2024, pp. 957-961, 958.

legislation such as the KoPl-G or the German NetzDG.[599/600] As one commentator noted, the CJEU effectively placed an exclamation mark after the country of origin principle.[601]

5.3.1.3. Relevance of the judgment for the interpretation of the DSA

Following the CJEU's findings, the KoPl-G was repealed in 2024 through the *DSA-Begleitgesetz* (DSA Accompanying Act – DSA-BegleitG).[602] The latter also introduced a number of amendments to existing Austrian legislation and established a new *Koordinator-für-Digitale-Dienste-Gesetz* (Digital Services Coordinator Act – KDD-G).[603]

According to Article 49 of the DSA, member states have to designate a national Digital Services Coordinator (DSC). In Austria, the *Kommunikationsbehörde Austria* (Communications Authority – KommAustria) was designated as the national DSC.[604] KommAustria[605] is the regulatory and supervisory body for broadcasting and electronic audiovisual media and would also have been in charge of enforcing the KoPl-G which was annulled by the CJEU as described above. It is supported in the tasks arising from the DSA by a branch of the regulatory authority organised as a private company fully owned by the state.[606]

Moreover, the KDD-G specifies a long list of administrative offences that providers of intermediary services commit by violating provisions of the DSA.[607] These administrative offences are punishable by KommAustria with a fine of up to 1% (for failure to supply information or submit to an inspection) or up to 6% (for all other offences) of the annual worldwide turnover of the provider in the preceding financial year.[608] If the requirements laid down in Article 51(3) (b) of the DSA are met, KommAustria shall request the *Bundesverwaltungsgericht* (Federal Administrative Court) to order temporary access restrictions to the service or, where that is technically not feasible, to the online interface.[609]

---

[599] On the German NetzDG see also Chapter 4.2.1.
[600] Liesching M., "*Das Herkunftslandprinzip limitiert Alleingänge nationaler Gesetzgeber: Anmerkung zu EuGH, Urteil vom 9.11.2023 – C-376/22*", *Zeitschrift für Urheber- und Medienrecht*, 2024, pp. 205 - 207, 207; Wimmer N. and Teetzmann C. "*Anmerlung zu Google Ireland and Others*, C-376/22", *MMR - Zeitschrift für das Recht der Digitalisierung, Datenwirtschaft und IT*, 2024, pp. 157-162, 162.
[601] Mantz R., "*Herkunftslandprinzip versus NetzDG – Wie geht es weiter mit den Pflichten von Diensteanbietern?" Zugleich Besprechung von EuGH "Google Ireland u.a.*", *Gewerblicher Rechtsschutz und Urheberrecht*, 2024, pp. 34-37, 37.
[602] Paragraph 10(1) Koordinator-für-digitale-Dienste-G, BGBl. I, Nr. 182/2023; for an English translation of the act, see RIS - ERV_2023_1_182 - Austrian Laws.
[603] For an overview in German, see Wittmann H., "*Das DSA-Begleitgesetz: Neue Instrumente zur Bekämpfung von 'Hass-im-Netz'*", *Medien und Recht*, 2023, pp. 298-301.
[604] Paragraph 2(1) *Koordinator-für-digitale-Dienste-G*, BGBl. I, Nr. 182/2023.
[605] See *Die Kommunikationsbehörde Austria* (KommAustria) | RTR.
[606] *Koordinator-für-digitale-Dienste-G*, paragraph 2(2); RTR Media | RTR.
[607] *Koordinator-für-digitale-Dienste-G,* paragraph 5.
[608] *Koordinator-für-digitale-Dienste-G,* paragraph 6.
[609] *Koordinator-für-digitale-Dienste-G*, paragraph 4.

5.3.2. The leeway for regulation of illegal online content after the CJEU ruling in *Google Ireland v. KommAustria*

The CJEU ruling in *Google Ireland v. KommAustria* remains relevant under the DSA "in so far as that regulation repeals neither the country of origin principle nor the possibility of derogating from that principle".[610] According to Article 2(3) of the DSA, that regulation does not affect the application of the eCommerce Directive, which remains in force. Consequently, the country of origin principle continues to apply.[611]

Moreover, Recital 9 of the DSA indicates that member states may regulate intermediary services under two conditions. First, the national measures must fall outside the scope of the DSA. Second, if they fall outside the scope of the DSA, they must still be in line with the country of origin principle of the eCommerce Directive. This entails that national regulation that extends to providers from other member states and falls outside the scope of the DSA, but inside the coordinated field of the eCommerce Directive, is only permissible if it is justifiable as an allowed derogation from the country of origin principle (and not harmonised by other EU legislation).

The ruling in *Google Ireland v. KommAustria* will further be relevant for interpreting the DSA, which also favours the principle of home member state control.[612] Under Article 56(1) of the DSA, it is generally the member state where the main establishment of the provider of intermediary services is located that has exclusive powers to supervise and enforce the DSA. Like the eCommerce Directive, the DSA views diverging national laws on intermediary services as threats to the free movement of these services.[613]

Within its scope of application, the DSA fully harmonises the rules applicable to intermediary services in the internal market (Recital 9 of the DSA). It is therefore no longer the member state of origin that determines these rules, but rather, this has been done by the EU.[614] In particular, the DSA establishes, according to its Article 1(2), a framework for the conditional exemption from liability of intermediary service providers, specific due diligence obligations for certain categories of intermediary service providers, as well as rules on the implementation and enforcement of the DSA. Conversely, the member states are free to regulate on matters that are not covered by the DSA. The DSA does not pre-empt any kind of national legislation concerning illegal online content.[615] In particular, the DSA does not define what is illegal online, but leaves this to the member states.[616] Moreover, national rules for illegal online content are permissible if they are pursuing other legitimate

---

[610] *Google Ireland v. KommAustria, Opinion of A.G. Szpunar* delivered on 8 June 2023, ECLI:EU:C:2023:467, paragraph 8; Liesching M., op. cit., pp. 205-207.
[611] Mischensky L., and Denk S., "*Digital Services Act und das Herkunftslandprinzip der E-Commerce-Richtlinie*", *Ecolex*, 2024(3), pp.226 *et seq*., 227.
[612] See Schroeder W., and Reider L., "*Der rechtliche Kampf gegen Hass im Netz - Nationale Spielräume unter dem DSA*", *Österreichische Jurist:innenzeitung*, 2024(8), pp. 465 *et seq*., 467.
[613] See DSA, Recitals 2, 4 and 9.
[614] Mischensky L., and Denk S., op. cit., pp. 226 *et seq*., 227.
[615] Schroeder W., and Reider L., op. cit., pp. 465 *et seq*., 467.
[616] Ibid, p. 468.

public interest objectives than those pursued by the DSA or implementing EU secondary legislation that remains untouched by the DSA.[617]

5.3.3. Application in view of cyber harassment and image-based sexual abuse

The bundle of legislative measures to combat hate on the Internet also contained amendments to a number of existing laws including several amendments to the Austrian *Strafgesetzbuch* (Criminal Code – StGB). Apart from the KoPl-G, the legislation on hate on the Internet remains largely valid.

Under the newly introduced criminal offences, a new offence of persistent cyber harassment has been established.[618] Cyber harassment can be either violations of the victim's honour or the dissemination of facts or images of the victim's most personal sphere without their consent. It is punishable if it is capable of unreasonably impairing the victim's way of life and perceivable by a large number of people over a long period of time. The penalty for persistent cyber harassment is imprisonment of up to one year or a monetary fine. The offence is punishable by imprisonment of up to three years if it results in the suicide or attempted suicide of the victim, or if it is committed continuously over a period exceeding one year or remains perceptible to the victim for more than one year.

Another major amendment to the StGB was the introduction of the offence of "upskirting".[619] "Upskirting" (or "downblousing") refers to the photographing or recording of a person's private parts without their consent, typically by aiming a camera up a skirt or dress. It is now punishable by imprisonment of up to six months or a monetary fine, irrespective of the eventual publication of the image recordings.

Furthermore, incitement to violence and hatred is now criminalised even if it is targeted not at an entire population group, but at an individual belonging to this group.[620] More recently, i.e. not by the *Hass im Netz-Bekämpfungsgesetz* but by a separate legislative initiative in 2025, a new offence was introduced to the StGB:[621] the unsolicited sending of images depicting exposed human genitals is now criminalised and subject to a penalty of up to six months' imprisonment or a monetary fine.

In addition to amendments to the StGB, other fields of law have been revised to improve the fight against hate on the Internet, in particular through changes to civil and criminal procedural law.

An amendment to the *Zivilprozessordnung* (Code of Civil Procedure – ZPO) aimed at the swift removal of online content that violates a person's human dignity.[622] If the alleged

[617] Ibid, p. 467. See DSA, Recital 9 (last sentence); Article 2(4).
[618] StGB, paragraph 107c; Article 8 of the *Hass im Netz-Bekämpfungsgesetz*, BGBl. I Nr. 151/2020.
[619] StGB, paragraph 120a; Article 8 of the *Hass im Netz-Bekämpfungsgesetz*, op. cit.
[620] StGB, paragraph 283; Article 8 of the *Hass im Netz-Bekämpfungsgesetz*, op. cit.
[621] StGB, paragraph 218(1b), introduced by the BGBl. I Nr. 45/2025.
[622] ZPO, paragraph 549, introduced by Article 3 of the *Hass im Netz-Bekämpfungsgesetz*, op. cit..

claim is sufficiently substantiated, the competent court has to issue an injunction order upon application of the plaintiff, without a prior oral hearing and without first hearing the defendant.

Furthermore, several amendments were made to the *Strafprozessordnung* (Code of Criminal Procedure – StPO). The first concerned the investigation of the accused person. Insult and defamation are private prosecution offences in Austria, which means that victims usually have to investigate the perpetrators themselves, often at considerable expense. The new procedure facilitates matters for victims.[623] Moreover, victims no longer bear the risks of costs in the event of an acquittal of the defendant.[624] Victims also get more psychosocial and legal support during proceedings.[625]

5.4. The example of Italy

Dr Giovanni de Gregorio, Professor in Law and Technology, Católica Global School of Law and Católica Lisbon School of Law

5.4.1. National legal framework concerning platforms

Growing awareness of the dangers of illegal content and disinformation has influenced Italy's online content regulations. While Italy's legal framework aligns with European law, especially considering the DSA, its enforcement primarily relies on national mechanisms. These include both administrative and judicial bodies, which are key in tackling illegal and harmful content such as hate speech and disinformation. Central to this system are not only courts, but also administrative authorities including the *Autorità per le Garanzie nelle Comunicazioni* (AGCOM) and other regulatory bodies that may be involved in specific cases concerning areas such as data protection or AI systems.

The DSA has replaced the patchwork of intermediary liability rules that member states had developed under the eCommerce Directive.[626] In Italy, the introduction of the DSA led to the partial repeal of the legislative decree[627] which had codified the earlier EU "safe harbour regime" with the liability privileges under the eCommerce Directive. Under the new DSA regime, the obligations governing online intermediaries in Italy, ranging from notice-and-action procedures for illegal content to enhanced transparency and accountability measures for VLOPs, are directly applicable, similar to other regulatory

[623] StPO 1975, paragraph 71; *Hass im Netz-Bekämpfungsgesetz*, op. cit., Article 10.
[624] StPO 1975, paragraph 390(1a); *Hass im Netz-Bekämpfungsgesetz*, op. cit.
[625] StPO 1975, paragraph 66b; *Hass im Netz-Bekämpfungsgesetz*, op. cit.
[626] Union European, 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 July 2000.
[627] *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 ellettronico* (Legislative Decree No. 70/2003).

instruments, such as the Regulation on Terrorism Content (TCOR),[628] the Regulation on Political Advertising (TTPAR),[629] and the European Media Freedom Act (EMFA).[630]

Furthermore, Italy has reformed its domestic media law through the *Testo Unico sui Servizi di Media Audiovisivi* (Consolidated Act on Audiovisual Media Services – TUSMA).[631] The TUSMA implements the revised AVMSD and extends regulatory obligations to "*fornitori di Servizi di piattaforma per la condivisione di video*" (providers of VSP services) encompassing services comparable to YouTube. These services are now subject to content standards, including rules on hate speech, the protection of minors, and incitement to violence. Such platforms are required to establish measures to limit the spread of hate and content that can be harmful to the public, for instance, by providing systems for flagging and reporting, ensuring transparent terms of service, or providing parental control tools.

5.4.2. Specific rules regarding defamatory, hateful and violence-inciting speech

The rules on hate speech and disinformation are not only connected to platform regulation, but also to criminal law and civil law. Particularly, according to the Italian *Codice Penale* (Criminal Code),[632] defamation occurs when someone harms another's reputation by communicating with at least two persons,[633] with aggravated penalties if the act is committed through the press or any other means of publicity. Italian courts have consistently held that the Internet, including social networks, constitutes such a means, thereby bringing online defamation within the aggravated form.[634] The penalties range from fines to imprisonment of up to three years, although imprisonment is increasingly substituted with pecuniary sanctions. The Criminal Code also addresses incitement to and apology for crime.[635] It addresses public instigation to commit offences and the glorification of criminal behaviour.

---

[628] European Commission, Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online, OJ L 172/79, 17 May 2021.
[629] European Commission, Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the transparency and targeting of political advertising, OJ L 2024/900, 20 March 2024.
[630] European Commission, Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L 2024/1083, 17 April 2024.
[631] *Decreto legislativo 8 novembre 2021, n. 208, attuazione della direttiva (UE) 2018/1808 del Parlamento europeo e del Consiglio, del 14 novembre 2018, recante modifica della direttiva 2010/13/UE, relativa al coordinamento di determinate disposizioni legislative, regolamentari e amministrative degli Stati membri, concernente il testo unico per la fornitura di servizi di media audiovisivi in considerazione dell'evoluzione delle realtà del mercato* (Legislative Decree No. 208/2021 – TUSMA).
[632] *Codice Penale* (Italian Criminal Code, approved by Royal Decree No. 1398/1930, as amended up to Legislative Decree 63/2018).
[633] Italian Criminal Code, Article 595.
[634] See, e.g. Italian Supreme Court, judgment 3453/2023; Italian Supreme Court, judgment 45680/2022.
[635] Italian Criminal Code, Article 414.

More specifically, provisions targeted at discriminatory expression emerged from the evolution of the Italian Criminal Code, the so-called Mancino Law,[636] which complements earlier anti-fascist and anti-racism legislation in Italy. Article 604-bis of the Criminal Code punishes propaganda based on the superiority or hatred of racial, ethnic, national, or religious groups, as well as incitement to discrimination or violence against such groups. Article 604-ter establishes an aggravating circumstance, increasing penalties when ordinary crimes are committed with discriminatory intent. These provisions are primarily connected to international human rights law and EU anti-discrimination law to address racist and xenophobic hate speech online. Other relevant legal examples can be found in Legislative Decree 215/2003,[637] implementing Directive 2000/43/CE,[638] implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, and Law No. 115/2016 against genocide and crimes against humanity.[639]

Disinformation, however, is not specifically regulated in Italy. Attempts to introduce legislation tackling online disinformation, including a bill to criminalise disinformation,[640] were not adopted. As a result, while combatting hate speech finds more legal grounds under criminal law and is reinforced through EU and other national regulatory frameworks, disinformation remains addressed only indirectly through platform regulation, media law obligations, or in cases where it overlaps with existing offences such as defamation or incitement to hatred.

5.4.3. Application in view of defamatory, hateful and violence-inciting speech

5.4.3.1. Administrative enforcement and the role of AGCOM

The administrative enforcement of content rules in Italy is under the competence of AGCOM. Its traditional mandate, including regulating telecommunications, broadcasting, and guaranteeing pluralism, competition, and the protection of minors,[641] has expanded over time towards online environments, initially from issuing non-binding codes of conduct and establishing observatories and monitoring systems to be designated as Italy's Digital Services Coordinator (DSC) under the DSA. These steps have contributed to transforming

[636] Italian Criminal Code, Articles 604-bis and 604-ter.
[637] *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* (Legislative Decree No. 215/2003).
[638] European Council, Council Directive 2000/43/EC of 29 June 2000, implementing the principle of equal treatment between persons irrespective of racial or ethnic origin, 2000, OJ L 180/22.
[639] *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* (Law No. 115/2016).
[640] Bill 2688.
[641] *Legge 31 luglio 1997, n. 249*, *Istituzione dell'Autorità per le garanzie nelle comunicazioni e norme sui sistemi delle telecomunicazioni e radiotelevisivo* (Law No. 249/1997).

AGCOM from a "communications watchdog" into the principal institutional actor for online content governance in Italy.

AGCOM's competence in Italy is limited to its national mandate. While the European Commission retains exclusive powers over very large platforms concerning systemic risks, AGCOM contributes to monitoring compliance and ensuring the enforcement of user rights at the national level. It also participates in the European Board for Digital Services (EBDS), where national authorities exchange information and develop common positions. AGCOM has responsibilities such as investigating breaches of the DSA, certifying out-of-court dispute resolution mechanisms, and coordinating with other national and European regulatory bodies.

AGCOM played an active role even before the adoption of the DSA. The authority adopted a regulation on the protection of human dignity, the principle of non-discrimination, and the fight against hate speech,[642] setting standards for all media to prevent discriminatory and offensive content and, with regard to VSP providers, promoting codes of conduct, identifying forms of co-regulation as well as mechanisms for oversight and monitoring of activities. This instrument was then complemented by another regulation[643] which aims to protect individual fundamental rights. That regulation expanded AGCOM's powers to combat hate speech. In particular, it establishes binding criteria that must guide the choices of providers of audiovisual media services, including video-sharing services, ensuring the prevention of incitement to violence and hatred. Furthermore, the regulation introduces a specific sanctioning mechanism, enabling AGCOM to impose monetary penalties whenever it ascertains a violation of the prohibition on incitement to violence or hatred against an individual or a group of persons on the grounds listed in Article 21 of the CFREU, or in breach of Article 604-bis of the Italian Criminal Code.

A more complex issue concerns disinformation. Considering the limited scope of Italian law in this regard, disinformation is addressed indirectly, through various approaches, including defamation and consumer law, consumer protection, copyright enforcement, or administrative measures. AGCOM's approach has been to promote media literacy, transparency of political advertising, and cooperation with platforms, rather than relying on criminal law. This regulatory framework can indeed also apply to situations where disinformation overlaps with hate speech concerning the same content. In fact, disinformation campaigns often exploit prejudices or discriminatory narratives, amplifying stereotypes or fuelling hostility against specific groups.

AGCOM has also engaged in soft enforcement through reports, guidelines, and multi-stakeholder fora. Since 2017 it has coordinated the *Tavolo per il pluralismo e la correttezza dell'informazione sulle piattaforme digitali*, a platform bringing together institutions, media, platforms, and civil society to address disinformation. Among these activities, AGCOM has conducted a fact-finding investigation on digital platforms and the information system, thus producing reports mapping the circulation of disinformation and analysing user perceptions and behaviour.[644] In addition, AGCOM adopted guidelines to

[642] AGCOM, Delibera 157/19/CONS.
[643] AGCOM, Delibera 37/23/CONS.
[644] AGCOM, Delibera 309/16/CONS; Delibera 79/20/CONS.

ensure equal access to online platforms during electoral campaigns,[645] developed within its technical round table, which promoted fact-checking tools and working groups on monitoring, classification, and media literacy.

5.4.3.2. Judicial enforcement and the role of courts

Courts are critical actors in the enforcement of the rules in disputes concerning illegal online content. Italian courts are regularly seized with cases of defamation and hate speech arising from platforms, particularly social media. This role is likely to increase considering the remedies introduced by the DSA for users to seek compensation.[646] Indeed, in addition to criminal liability, victims may pursue civil remedies such as damages, based on a general principle of liability for damages caused by unlawful conduct,[647] or access preliminary injunction mechanisms. Courts may award compensation and order corrective measures, such as the removal of the defamatory content.

Courts continue to apply the same system of intermediary liability based on the liability limitations as maintained in the DSA, for example in the case of the responsibility of social media, and, also, bloggers for third-party content.[648] In that regard, the Italian Supreme Court has focused on distinguishing between passive and active providers,[649] and reaffirmed the liability of online content providers for defamatory material when they fail to promptly remove it after being notified.

Nonetheless, courts have addressed similar cases on online hate speech in different ways, as in the divergent rulings on Facebook's removal of far-right parties CasaPound and Forza Nuova in 2019.[650] While CasaPound initially won an injunction from the Rome Tribunal ordering Facebook to restore its page, with the court reasoning that deplatforming an otherwise legal political party violated constitutional rights to expression and participation in politics, by contrast, Forza Nuova's claim was rejected from the outset in 2020, with the court holding that its racist and fascist content clearly breached Facebook's terms of service and that spreading hate is not a right. However, after a full trial in 2022, CasaPound's content was considered hate speech outside the protection of freedom of expression, and thus Facebook was regarded as having lawfully disabled the accounts. Together, these cases highlight the tension in Italian jurisprudence between safeguarding political pluralism and affirming the contractual right and duty of platforms to remove hate speech.

At the same time, courts have confirmed the responsibility of users as primary infringers, particularly in the case of defamatory posts on social media. Nonetheless, the challenge is to balance freedom of expression with other conflicting constitutional interests. For instance, in a case involving a woman convicted for Facebook posts deemed

[645] AGCOM, *Linee guida per la parità di accesso alle piattaforme online durante la campagna elettorale per le elezioni politiche 2018* (Guidelines for equal access to online platforms during electoral campaigns 2018).
[646] Article 54 of the DSA.
[647] Article 2043 of the Italian Civil Code.
[648] Italian Supreme Court, judgment 17360/2025.
[649] Italian Supreme Court, judgment 39763/2023.
[650] Court of Rome, Order 59264/2019; Court of Rome, Order 64894/2019.

damaging to a municipal councillor's reputation, the Italian Supreme Court overturned the conviction, affirming that even strongly worded or vulgar commentary may be lawful if it constitutes a valid exercise of the right to critique.[651] The key condition is that such expressions remain proportionate, contextually appropriate, and do not amount to gratuitous personal attacks or humiliations. However, in another case, involving the dissemination of defamatory comments by a former municipal assessor, the court ruled that the use of offensive language and personal insults exceeded the limits of legitimate political criticism, affirming the application of defamation laws in such contexts.[652]

Courts face challenges in addressing disinformation because legal remedies are inherently reactive, requiring proceedings that take time to resolve, while online falsehoods can spread rapidly and irreversibly. Moreover, the lack of a dedicated legal framework for this type of content means that judges must rely on existing provisions such as defamation or hate speech, which may not always easily apply to disinformation. This creates uncertainty in legal interpretation and uneven enforcement. Even after the adoption of the DSA, which establishes procedural mechanisms for tackling illegal content, the scale of online disinformation, particularly in the case of campaigns, could challenge judicial remedies.

5.4.3.3. Challenges in national enforcement

Italy's regulatory framework for online content aligns closely with EU law, particularly through the DSA, and is complemented by domestic instruments such as the TUSMA and the Mancino Law. Together, these measures establish a system in which AGCOM exercises administrative oversight while courts provide judicial remedies, addressing issues such as hate speech and other forms of illegal content through regulatory, civil, and criminal mechanisms. This layered approach is primarily rooted in EU law, which also shapes national enforcement pathways.

Challenges arise, however, in the area of disinformation. As in other member states, Italy relies on indirect regulatory tools, judicial remedies, and platform-led initiatives. These mechanisms are less effective in responding to the speed and scale at which disinformation circulates online. While administrative authorities are increasingly called on to address the circulation of illegal content while operating within the limits of their mandates, effective responses at national level increasingly depend on coordination between national regulatory authorities and European institutions through the EBDS, particularly in addressing disinformation as a systemic risk.

[651] Italian Supreme Court, judgment 22341/2025.
[652] Italian Supreme Court, judgment 11571/2025.

6. Other areas of harmful content: enforcement by restrictions

6.1. Enforcement at EU level

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

While the preceding chapters have primarily addressed enforcement mechanisms for the removal of, or disabling of access to, illegal content, this chapter shifts the focus toward content that is not necessarily unlawful but may nonetheless be subject to access restrictions for specific groups, in particular minors, as the content may be harmful to them.[653] A notable example is pornographic content, which, although not prohibited per se under most national legal systems, is generally subject to limitations when it comes to its accessibility by minors.[654] In this context, regulatory regimes have emerged that do not criminalise the content itself but rather seek to control its accessibility based on the risk and potential harm it may pose to vulnerable audiences.

Within the European Union, such protective measures are most clearly articulated in the AVMSD. The AVMSD establishes a harmonised framework that requires member states to ensure that audiovisual media services do not include content that may impair the physical, mental, or moral development of minors, unless such content is made available in such a way that ensures minors will not normally hear or see it. As outlined in Chapter 2.2.2, the AVMSD applies both to traditional broadcasting and to on-demand services, as well as in parts – including the obligation to protect minors – to providers of VSP services, reflecting the increasing convergence of media consumption patterns. Measures under the AVMSD may include technical access restrictions, age verification tools, and the use of classification systems or descriptors to inform viewers, for VSPs the measures that member states may impose on them are listed in detail in the Directive. These measures to protect minors at national level in the EU member states have been dealt with in the recent *AVMSDigest – Safe Screens: Protecting minors online*[655] by the European Audiovisual Observatory (EAO), so this report will focus on restrictions under the DSA framework. Overall, it can be observed that while the AVMSD sets out content-specific rules for audiovisual media services, particularly in relation to minors and in some cases for the

[653] For the definition of harmful content in this context; see Lacourt A., Munch E., Radel-Cormann J., *AVMSDigest, Safe Screens: Protecting Minors Online*, European Audiovisual Observatory, Strasbourg, October 2024, pp. 13 ff.
[654] For more details and a country comparison see Ukrow, J., Cole, M.D. and Etteldorf, C., *Stand und Entwicklung des internationalen Kinder- und Jungedmedienschutzes*, EMR Script Bd. 7, dco-Verlag, Püttlingen, 2023 (with an English summary, pp. 34ff.). See also, Verdoodt, V., Lievens, E. and Chatzinikolaou, A., "The EU Approach to Safeguard Children's Rights on Video-Sharing Platforms: Jigsaw or Maze?", *Media and Communication* 11(4), 2023, pp. 151-163.
[655] Lacourt, Munch and Radel-Cormann, op. cit. See also in detail Weinand, J., *Implementing the EU Audiovisual Media Sevices Directive*, Nomos, Baden-Baden, 2018, especially pp. 489 ff and 741 ff.

general public, the DSA complements this by addressing the broader ecosystem of digital content dissemination, especially through VLOPSEs, ensuring that protective measures are embedded into the architecture of online services more generally.

The DSA as a European regulation introduces a horizontal framework for regulating online intermediaries which has been outlined in Chapter 2.2.2. While the DSA does not directly impose bans on certain content, it assumes that providers of intermediary services, similar to the AVMSD, apply mechanisms through which access to content may be restricted, particularly where such content is harmful for vulnerable recipients of the service such as minors. The protection of minors is an important policy objective of the European Union[656] and has been explicitly incorporated into the DSA. Namely, under Article 28(1) of the DSA, platforms which are accessible to minors – which in principle means all publicly accessible online platform services without a specific access condition and therefore has a very broad scope of application – are required to take appropriate and proportionate measures to protect minors.[657] Such measures can include designing the platform interfaces or parts thereof with the highest level of privacy, safety and security for minors by default, where appropriate, or adopting standards for the protection of minors, or participating in codes of conduct for protecting minors.[658]

Harmful content and its impact on minors further constitutes one of the systemic risks that VLOPSEs have to consider within their systemic risks assessment and need to mitigate according to Article 35(1) of the DSA.[659] Related systemic risks may also arise from the design, functioning or use, including through manipulation, of VLOPSEs, with actual or foreseeable harm to public health, minors and individual physical and mental well-being.[660] Mitigation measures must be reasonable, proportionate and effective and tailored to the specific systemic risks; these may include age-appropriate content curation, parental control tools, and transparent default settings. In selecting the appropriate mitigation measures, providers can consider, where appropriate, industry best practices, including as established through self-regulatory cooperation, such as codes of conduct. In addition, they should take into account the guidelines from the European Commission.[661]

These guidelines concerning Article 28 of the DSA were published by the European Commission in July 2025 with the aim of helping online platforms in their efforts to comply with the obligation resulting from Article 28 of the DSA to enhance privacy, safety and security for children online.[662] The guidelines set out a non-exhaustive list of recommended

---

[656] DSA, Recital 71.

[657] On the proportionality of such measures see Liesching M., "Artikel 28 DSA" in Liesching M. (ed.), op. cit., paragraphs 38 ff. Generally, Wilman, F., Kalėda, S.L. and Loewenthal, P.J., *The EU Digital Services Act,* Oxford University Press, Oxford, 2024, p. 218.

[658] Ibid.

[659] On the protection of minors under the DSA see Buiten, M., Ledger, M. and Busch, C., *Future of the DSA: Safeguarding Minors in the Digital Age*, DSA Implementation Forum, March 2025.

[660] Recital 83 of the DSA.

[661] Recital 89 of the DSA.

[662] European Commission, "Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065", 2025; the Draft Guidelines

measures that platforms can implement to protect minors. These measures are grounded in the principle of privacy by design and advocate for a default settings approach that prioritises child safety. Consistent with the DSA's overarching risk-based approach, the guidelines acknowledge first of all that platforms present varying levels of risk to minors. This allows for flexibility in implementation, enabling the providers to tailor protective measures to their specific services while avoiding unnecessary restrictions on children's rights to participation, access to information, and freedom of expression. Accordingly, any measure that a provider of a platform accessible to minors puts in place to comply with Article 28(1) of the DSA must adhere to the following general principles: the principle of proportionality, respect for children's rights, privacy-, safety- and security-by-design and age-appropriate design.[663]

One of the main approaches recommended concerns the implementation of age assurance mechanisms to limit children's exposure to age-inappropriate content. However, before such a mechanism is put in place, the provider should consider whether the aim of a high level of privacy, safety and security for minors on their service may be achieved already by relying on other less far-reaching measures.[664] The European Commission considers the use of an age verification method to be an appropriate and proportionate measure where applicable EU or national law prescribes a minimum age to access certain products or services offered and/or displayed on the online platform (such as the sale of alcohol, access to pornography, or access to gambling content). The same applies to instances where the terms and conditions or any other contractual obligations of the service require a user to be 18 years of age or older to access the service, as well as scenarios where the provider has identified risks for minors that cannot be mitigated by other less intrusive measures. It must be noted that the issue of age verification is complex and has been discussed for a long time also in view of practical – including enforcement – challenges.[665]

Even though the respective provisions in both the AVMSD and the DSA clearly acknowledge the need to protect minors and corresponding efforts by the platforms, there remain questions for the providers regarding what level of age verification would be considered sufficient when deciding about the implementation of protective measures for minors. For instance, the AVMSD requires content which can be harmful to minors to be

---

were open for public feedback from 13 May to 10 June 2025 and were approved on 14 June 2025; see European Commission, Annex to the Communication to the Commission, Approval of the Content on a Draft Communication from the Commission- Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online, pursuant to Article 28(4) of Regulation (EU) 2022/2065. See also Munch, E., "European Commission Publishes Guidelines on the Protection of Minors under the DSA", IRIS 2025-8/9, European Audiovisual Observatory, 2025. For an assessment from a data protection perspective see Stalla-Bourdillon S., "A GDPR Lens on the Draft Article 28 DSA Guidelines and Their Approach to Age Assurance", *European Data Protection Law Review*, 2025, 11(2), pp. 207-214.

[663] See European Commission, "Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065", op. cit., pp. 6 ff.

[664] Ibid., p. 9.

[665] See OECD, "The Legal and Policy Landscape of Age Assurance Online for Child Safety and Well-Being", OECD Technical Paper, June 2025. For an overview on age verification and parental control mechanisms implemented see Broughton Micova S., and Kostovska, I., *The Protection of Minors on VSPs: Age Verification and Parental Control*, European Audiovisual Observatory, Strasbourg, 2023. As regards enforcement challenges, see for instance Schmitz-Berndt, S., "Berlin Administrative Court Rejects Application for Interim Legal Protection of Porn Platforms against Media Authority Blocking Order", op. cit.

disseminated in a way that is not "normally" heard or seen by this age group without mandating specific age verification technologies. Similarly, Article 28(1) of the DSA requires the implementation of "appropriate and proportionate measures" reaching a "high level of … safety", without further detailing what a high level may constitute.

The European Commission's guidelines, even if not legally binding as such, give much more specific suggestions on new standards for age verification tools to the providers. They consider the forthcoming EU Digital Identity Wallet[666] as an appropriate and reliable means of digital identification under the DSA. The wallet, which member states have to introduce by 28 November 2026, will serve the purpose of a harmonised digital identity framework and allow the registering of age information in a centralised way. This information would then be accessible only for verification of whether or not a user who is, for example, requesting access to a website, falls into the category of not being a minor, without any further granularity, e.g. regarding the exact age or personal data of the subject concerned. However, before the Digital Identity Wallet becomes available, the European Commission has published, together with the guidelines, an open-source age verification solution, including a dedicated app, as a standalone measure, which it suggests could become an EU-wide "benchmark for a device-based method of age verification".[667] As with the EU Digital Identity Wallet, in the future, this system would ensure that besides the age check, no further details would be revealed and the platforms asking for verification of the age would only receive the information that the user is aged over 18.

Age estimation is to be distinguished from age verification. Such a measure only serves to reach an approximation of the user's age, in other words, confirmation that a user is likely to be of a certain age.[668] The guidelines list circumstances under which estimation methods will suffice, such as where the provider has identified in its risk review at most medium risks to minors on their platform and the restriction should not apply to all minors under 18, but only to younger age groups. In contrast, the European Commission considers that self-declaration, meaning that the individual supplies his or her age him/herself, does not meet the criterion of an effective age assurance method.[669]

It is notable that the first DSA enforcement actions by the European Commission related to potential violations of protection-of-minors obligations. It has so far taken several actions against VLOPs for non-compliance with provisions protecting minors from harmful content. For instance, in May 2025, it opened formal proceedings against providers of pornographic content, namely the providers of Pornhub, Stripchat, XNXX, and XVideos which had been designated as VLOPs.[670] The European Commission's investigations focus on the risks of these types of services for minors, including those linked to the absence of effective age verification measures. For instance, the proceedings against Pornhub were

---

[666] The framework mandating member states to provide EU Digital Identity Wallets to citizens is Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending Regulation (EU) No. 910/2014 as regards establishing the European Digital Identity Framework, OJ L 2024/1183, 17 April 2024.

[667] European Commission, Commission Guidelines on Measures to Ensure a High Level of Privacy, Safety and Security for Minors Online Pursuant to Article 28(4) of Regulation (EU) 2022/2065, op. cit., p. 10.

[668] Ibid., p. 9.

[669] Ibid., p. 15.

[670] European Commission, "Commission Opens Investigations to Safeguard Minors from Pornographic Content under the Digital Servcies Act", Press release, 27 May 2025.

based on the preliminary finding that the provider was in breach of Articles 28(1), 34(1), 34(2) and 35(1) of the DSA, which included that the provider, Aylo, offering this service had used a self-declaration method as an age assurance method to restrict access to the service for minors.[671] The opening of formal proceedings empowers the European Commission to take further enforcement steps, such as adopting interim measures and non-compliance decisions. In parallel to and complementing the enforcement activities of the European Commission, the member states in the EBDS became active against smaller platforms providing pornographic content, which have not been designated as VLOPs and for which national authorities remain competent. The member states launched a coordinated action to ensure a consistent and efficient application of the DSA across the EU,[672] after individual member states had previously already initiated actions.[673]

6.2. The example of Poland

Dr Krzysztof Wojciechowski, Legal Adviser, Adviser to TVP, Chair of the Copyright Committee in Poland, Lecturer in Post-Graduate Studies on Intellectual Property, University of Warsaw

6.2.1. National legal framework concerning platforms

Poland has been an example of a country where debates about the freedom of Internet are particularly intense, especially in connection with initiatives concerning the regulation of online activities, such as those in the field of copyright and/or media law.[674]

Notably, the legal framework concerning online platforms in Poland is not yet complete as the implementation of the Digital Services Act (DSA)[675], adopted on 18

[671] European Commission, Case DSA.100059 – Pornhub – Investigation into Compliance with Articles 28(1), 34(1), 34(2) and 35(1) of Regulation (EU) 2022/2065, 27 May 2025.
[672] European Commission, "The European Board for Digital Services Launches a Coordinated Action to Reinforce the Protection of Minors as regards Pornographic Platforms", Press release, 27 May 2025.
[673] See for instance Schmitz-Berndt, S., "Berlin Administrative Court Rejects Application for Interim Legal Protection of Porn Platforms against Media Authority Blocking Order", op. cit.
[674] One earlier example is Polish action for annulment of Article 17(4) c) and d) *in fine* of the Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, OJ L 130/92, 17 May 2019, in the light of Article 11 of the Charter of Fundamental Rights of the EU, resulting in the CJEU judgement of 26 April 2022 (C-401/19 *Poland v. European Parliament and Council of the EU*, ECLI:EU:C:2022:297).
[675] 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 (DSA), OJ L 277, 27 October 2022.

December 2025 by the Parliament,[676] was vetoed by the President on 9 January 2026.[677] Even before parliamentary proceedings began and then in Parliament, a part of the political scene, some stakeholders, NGOs and other bodies voiced concerns that the proposed model of preventive orders, in particular regarding hate speech, could lead to "Internet censorship".[678] The evolution of the draft through the governmental and then parliamentary sessions was in large part aimed to respond to these concerns. Despite these, the President still contested the risk for freedom of expression and refused to sign the act adopted by the Parliament.

The implementation of the DSA was to take the form of a comprehensive revision of the *Ustawa o świadczeniu usług drogą elektroniczną* (Act on provision of services by electronic means - UŚUDE).[679] With regard to institutional solutions, the amending Act designates the telecommunications regulator, the *Urząd Komunikacji Elektronicznej - Prezes* (President of the Office of Electronic Communication - UKE) as the national Digital Services Coordinator (DSC) and supervision authority. Exceptions apply regarding e-commerce platforms and consumer protection, which shall be supervised by the competition authority – the President of the Office of Competition and Consumers Protection, the *Urząd Ochrony Konkurencji i Konsumentów* (UOKiK), and to video sharing platforms (VSPs), which shall be subject to the competences of the media regulator (Chair of the National Broadcasting Council – *Krajowa Rada Radiofonii i Telewizji* - KRRiT). The act also provides for rules and procedures for the President of the UKE to grant the status of trusted flaggers and vetted researchers, as well as for the certification of bodies for out-of-court dispute settlement. The revision further establishes procedures for the supervision of compliance with the DSA, for administrative penalties in the event of breaches, and for the handling of complaints provided for in Article 53 of the DSA; it also provides for rules of civil liability for DSA infringements and related court proceedings.

The most significant and debated changes to the act are the rules and procedures for orders to act against illegal content and, though less controversially, orders to restore content that has been erroneously removed.[680] The concept of illegal content has

---

[676] *Ustawa z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną i niektórych innych ustaw* (The act of 18 December 2025 amending the act on provision of services by electronic means and some other acts). The evolution of the draft during governmental works and consultations are documented *here*. The parliamentary works on the governmental draft in the *Sejm* [lower house] and the Senate's resolution.

[677] The motion by the President of 9 January 2026 to reconsider the act of 18 December 2025 amending the act on provision of services by electronic means and some other acts

The *Sejm* may adopt the act again (reject the veto) with 3/5 majority (Article 122 paragraph 5 of the Constitution). This is however unlikely given that fewer votes supported the act in the vote in the *Sejm*.

[678] The divide may be illustrated by the voting results in the *Sejm* on 21 November 2025, when the act was supported by 237 votes, mainly of the governing coalition (KO, PSL, Polska 2050, Lewica), while 200 of the opposition (PiS, Konfederacja) were against and 5 abstained The diverging views were presented during the public hearing in the *Sejm* on 4 November 2025. The draft was supported by IP rights holders, including film and music producers, CRMOs and press publishers. Some civil society organisations noted the positive evolution of the draft (e.g. the Helsinki Foundation of Human Rights, Panoptykon), while some others (e.g. *Ordo Iuris*, the Society of Polish Journalists and the Chair of KRRiT) raised the risk of abuse, of blocking orders to censor the Internet. ;

[679] *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Act of 18 July 2022 on the provision of electronic services), consolidated text: *Journal of Laws* (*Dziennik Ustaw*) of 2024, item 1513.

[680] Chapter 2a (Articles 11a-11u) of UŚUDE, as added by the amending act of 18 December 2025.

significantly evolved during governmental work on the draft. Initially, the draft referred to illegal content without defining it. Following consultations, the text referred broadly to infringements of personality rights, intellectual property rights, criminal offences and infringements of consumer protection. The draft submitted by the government to the parliament and adopted by it is considerably more limited in scope and at the same time more precise, referring to a closed catalogue of 27 criminal offences.

According to the statement of reasons accompanying the draft submitted by the government, there are three criteria for identifying a specific infringement: 1) it must occur online – taking into account the *modus operandi* of the perpetrator; 2) it must take into account how the content is disseminated; 3) blocking access to the content must not cause negative consequences for democratic discourse and elections. Listed offences include, in particular: punishable threats; incitement to suicide or self-harm; human trafficking; abuse of another's image; the unauthorised circulation of naked or sexual images; the dissemination of pornography enabling access to minors under 15 years of age; contacting such minors online to commit a sexual crime; the promotion of paedophilia; the dissemination of pornography involving minors, animals or violence; false alarms activating public institutions; the promotion of totalitarianism; incitement to hatred on racist, xenophobic or religious grounds; public insult on such grounds; fraud; copyright infringement through unauthorised dissemination of a work; or the remote sale of tobacco. The scope of illegal content is not limited to materials that directly constitute the offences listed, but also content inciting the commission of such acts.[681] The act exempts cases governed by *leges speciales*, *i.e.* terrorist contents; terrorist or espionage related IT data; breaches of consumer protection law; programmes, videos or other content which is non-compliant with rules of the *Ustawa o radiofonii i telewizji* (Broadcasting Act)[682] on VSP services (Article 47o) concerning the protection of minors, counteracting incitement to violence and hatred, and/or content facilitating terrorism, pornography involving minors, or racist, xenophobic or religious insults.

According to the adopted but vetoed act, motions for orders to prevent access to illegal content within a service provided by an intermediary service provider were to be submitted by a public prosecutor, the police,[683] a body of the *Krajowa Administracja Skarbowa* (National Revenue Administration - KAS), a copyright or related right-holder, or a service recipient.[684] Such motions were to be examined, and orders issued, by the Chair of KRRiT for content on VSP services and by the President of the UKE for all other content. Proceedings would be expedited, with decisions due within two days for motions from

[681] The governmental draft and the act adopted initially by the *Sejm* referred also to content "praising" such offences, Senate's amendments removed this as unclear and disproportional, while potentially affecting the freedom of expression; e.g. doubts were raised whether likes or links to illegal content may constitute "praising" it.

[682] *Ustawa z dnia 29 grudnia 1992 r. o radiofonii i telewizji* (The Broadcasting Act), consolidated text, Journal of Laws (*Dziennik Ustaw*) of 2022, item 1722, with amendments; English translation.

[683] In cases concerning human trafficking, also the border guard.

[684] The governmental draft proposed to also entitle trusted flaggers to submit such motions. This was criticised by the opponents of the draft, as allegedly bringing the risk of some organisations with the status of trusted flaggers submitting motions for orders with political or ideological motivation. The Parliament, following Senate's amendments, decided finally to remove trusted flaggers from the list of bodies and entities entitled to submit motions. Instead, copyright and related right-holders were added to the list.

prosecutors or police, seven days in other cases, and 21 days for particularly complex matters. Deadlines would run from the expiry of the two-day period granted to the uploading recipient to present their position. For motions by service recipients seeking the removal of hosting restrictions under Article 17(1) of the DSA, decisions would be issued within 14 days under similar procedural rules. It would be possible for parties to file a court objection via the issuing authority within 14 days; the court would apply non-litigious civil procedures, and its rulings would be subject to appeal, including cassation. Decisions on orders would not be declared immediately enforceable, but only after the objection deadline, if no objection had been filed.[685] The registry of Internet domains used to disseminate illegal content was to be run by the President of the UKE to list domains which lacked effective measures to enforce orders, and providers of Internet access services would have been obliged to disable access to web pages using listed domain names and redirect users to the web page of the UKE.

The proposed mechanism for preventive orders has been a matter of controversy throughout the drafting of the DSA implementation bill. Critics have particularly pointed to the alleged vagueness of the criteria in some cases, and the risk of subjective judgments, in combination with the fact that the competences to issue such orders would rest with the governmental regulatory authority (the President of the UKE appointed by the *Sejm* on the motion of the Prime Minister). These concerns have been framed as potentially leading to censorship. Following the narrowing and clarification of the definition of "illegal content", replacing the earlier broad reference to any infringement of personality rights or IP rights, the criticism focused on certain listed criminal offences, often collectively referred to as "hate speech", for allegedly giving rise to the mentioned risks. The proponents of the draft, in turn, stress the precise listing of types of illegal content linked to relevant serious criminal offences, and the safeguarding of the judicial review of preventive orders.[686] Further steps to mitigate concerns were taken in the *Sejm* and Senate during the parliamentary sessions, including some guarantees of apoliticality, impartiality and fairness of persons examining motions for orders; removal of trusted flaggers from the entitled entities list; lack of immediate enforceability of orders; and removing the "praising" of listed criminal offences as a possible reason to justify removal.[687] These steps were found insufficient by the President, who refused to sign the act. The statement of reasons for the presidential motion to reconsider the act notes the political divide over the act in the Parliament and hence lack of consensus; while the defined list of criminal offences is praised, certain offences, such as infringements of IP rights, is seen as requiring further judicial assessment. The passing of competence to block contents to "governmental executive bodies", such as the President of the UKE, without prior judgement by the court is criticized in the light of freedom of expression, given the risk of political influences. Also,

[685] Lack of enforceability of orders before the deadline for judicial review was another amendment by the Senate in response to concerns about the alleged risk of online censorship by state bodies. The governmental draft and the act adopted initially by the *Sejm* were to allow declaration of immediate enforceability of orders, if justified by the scale of the harm or public interest.

[686] *Ministerstwo Cyfryzacji*, *"Nowe zasady w Internecie — sprawdź, co zmieni DSA"*, (New rules on the Internet – Find out what the DSA will change), 3 November 2025, Ministry of Digital Affairs government portal

[687] Cf., e.g. Article 11c, Article 11a, paragraph 1, Article 11n, UŚUDE as added by the amending act of 18 December 2025. For the justification of amendments by the Senate – cf. the statement of reasons for its resolution of 10 December 2025

the proportionality of administrative blocking of content is questioned, as this is not required as such by the DSA and there exist other available measures, such as the "notice and action" mechanism and/or court proceedings with the request for interim relief (e.g. an order for temporary removal of contents). Both the lack of enforceability of orders prior to judicial review, and lack of urgent procedures allowing the court to review objections are criticised as potentially leading to the ineffectiveness of the mechanism.[688] It remains to be seen how things will develop, whether, in the likely case that there is no rejection of the veto by the *Sejm*, the initiative will come back in the changed form or with the reduced scope.

Beyond the implementation of the DSA, the existing national legal framework relevant to online platforms consists mainly of provisions of the UŚUDE, which implements the eCommerce Directive[689] and largely reflects the directive's structure and content. The UŚUDE defines relevant notions, in particular the provision of services by electronic means. It declares that such services are subject to the law of the member state of the EU or EFTA/EEA in which the service provider has their headquarter or residence (country of origin principle), with certain exceptions (e.g. protection of intellectual property) and possible limitations, subject to the specified procedure based on Article 3(4) and (5) of the eCommerce Directive.[690] Furthermore the UŚUDE provides for the duties of service providers regarding information allowing identification, terms and conditions, as well as commercial communications and personal data. Further, the UŚUDE still contains provisions on liability exemptions for providers of mere conduit, caching and hosting services and the principle of no general monitoring duty; these provisions will be repealed, given that these matters are now regulated directly in Chapter II (Articles 4-8) of the DSA.

An important exception to the country of origin principle for online services concerns online gambling. Such services are subject to Polish law, if the gambling game is organised within the territory of Poland, the service recipient takes part in the game within this territory and/or the service is targeted at recipients in Poland, notably when it is available in Polish language and/or advertised in Poland.[691] Detailed duties of online gambling organisers are set out in *ustawa o grach hazardowych* (Act on gambling games)[692] which aims to protect participants from negative consequences of gambling. These measures include, *inter alia,* a ban on participation by individuals under 18, age verification procedures, as well as protections for minors in the context of online gambling advertising. The Minister of Finance maintains a register of domains offering online gambling games that do not comply with the law and are accessible in Poland. Telecom operators providing access to internet services must prevent access to the web pages using domain names listed in the register. Further, the provision of payment services for such web pages is forbidden.

---

[688] Also the possibility for grants from the state budget to trusted flaggers as leading to "conflict of interest" diminishing their independence is referred to as another reason for the veto.

[689] European Parliament and EU Council, Directive 2000/31/EC of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market OJ L 178, 17 July 2000.

[690] Articles 3a and 3b, UŚUDE. Interestingly, the act of 18 December 2025 amending UŚUDE (aimed to implement DSA) and vetoed by the President was to add orders to act against illegal content and restore content to the list of exceptions from the country-of-origin principle (Article 3a paragraph 2, UŚUDE).

[691] Art. 3a[1] of the UŚUDE.

[692] Sejm, *Ustawa z dnia 19 listopada 2009 r. o grach hazardowych* (Act on Gambling Games of 18 November 2009), consolidated text: Journal of Laws (*Dziennik Ustaw*) of 2025, item 595; cf. Articles 15d – 15i.

This mechanism served as inspiration for the recent legislative drafts on the protection of minors against harmful content/pornography, which will be discussed below.

The existing legal framework for online platforms also includes provisions in the Broadcasting Act on VSPs[693] implementing Articles 28a and 28b of the Audiovisual Media Services Directive – AVMSD).[694] Among the regulated matters are the criteria for Polish jurisdiction over VSPs; duties of transparency, including with regard to the ownership structure of providers; the list of VSPs run by the media regulator, KRRiT; and the duty of providers to notify their VSPs to KRRiT. With regard to content on VSPs, providers are obligated to apply measures preventing the dissemination of content harmful to minors, inciting violence and/or hatred, facilitating terrorist crimes, inciting racist or xenophobic insults, and including pornography involving minors. Moreover, such providers shall offer users mechanisms to report violations of rules on harmful or illegal content and respond to users within 48 hours. Disputes concerning the handling of such reported violations may be resolved by mediation. If the violation is not remedied by the uploading user within a specified period of time, the VSP provider shall prevent access to the non-compliant content.

The Terms and conditions of online services offered by VSP providers should specify the conditions for the classification and marking of content, the rules for commercial communications, the procedures for reporting on content harmful to minors, and the criteria for assessing compliance with rules regarding harmful content; they should also include information on the lodging of complaints against preventing access to users' contents and on the processing of personal data.

The provider may suspend a user from uploading content in the event of repeated violations, despite a prior request to cease such conduct. In general, the suspension may last for three months, but if breaches concern the facilitation of terrorism, pornography involving minors, or incitement to racist insults, the suspension may be imposed permanently. Any such decisions by the VSP provider should include justification and may be subject of a complaint to KRRiT. The Chair of KRRiT is empowered to issue decisions ordering the restriction of access to any content on the VSP that violates the rules on harmful or illegal content, but also to restore access to content uploaded by a user or to reinstate a user's ability to upload content on the platform. Similarly to providers of media services, VSP providers have the duty of evidence retention, i.e. they shall retain copies of contents for 28 days from the date of removal from the platform and present these to the Chair of KRRiT upon request.

---

[693] Chapter 6b, Articles 47l – 47w, Broadcasting Act, op. cit.

[694] European Parliament and of the EU Council Directive 2010/13/EU of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (AVMSD), OJ L 95/1, last amended by 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 November 2018, as well as by Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act), OJ L 2024/1083, 17 April 2024.

The provisions of the Broadcasting Act regarding on-demand audiovisual media services (AVMS)[695] may also be relevant to the content offered on VSPs, including those outside Polish jurisdiction, as channels on platforms with catalogues of video content, run as business, are considered media services. In consequence, the list of on-demand AVMS providers managed by KRRiT contains over 900 services, in large part those available on YouTube, X , Facebook, Instagram or TikTok.[696] In contrast, KRRiT's list of VSP providers, to which the Broadcasting Act applies, contains only 14 services.[697] The regulation of on-demand AVMS in Poland is largely based on the AVMSD.[698] However, providers of such services, in addition to a basic identification duty, are also subject to an ownership transparency obligation, which extends to their other media services. Providers of on-demand AVMS are required to apply for registration in the list of VOD providers managed by KRRiT and must submit to KRRiT annual reports on compliance with provisions on the protection of minors, the promotion of European works, and accessibility for persons with disabilities. If content harmful to minors has been provided without technical safeguards or other protective measures at least twice within 12 months, the Chair of KRRiT may (after an ineffective request to cease such practices), by a formal decision, remove the provider of the service in question from the list.

6.2.2. Specific rules to protect minors from online harm in the Broadcasting Act

A specific set of rules to protect minors from harmful content is provided for in the Broadcasting Act, covering linear programme services (radio and television), including those transmitted online,[699] and also, as already outlined, on-demand AVMS[700] and VSPs.[701]

With regard to linear programme services and on-demand AVMS, the law distinguishes between content that is "prejudicial to the physical, mental or moral development of minors", in particular content containing pornography or gratuitous violence, and content that "may have an adverse impact upon the healthy physical, mental or moral development of minors", which is only likely to have such a negative impact.[702] The

[695] Chapter 6a, Articles 47a-47k, Broadcasing Act, op. cit.
[696] The list by the Chair of KRRiT of providers of on-demand audiovisual media services (VOD) – 4 August 2025 (*Lista dostawców audiowizualnych usług medialnych na żądanie (VOD) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)
[697] The list by the Chair of KRRiT of VSPs providers – 4 August 2025 (*Lista dostawców Platform Udostępniania Wideo (VSP) wpisanych do wykazu Przewodniczącej KRRiT stan na 4 sierpnia 2025 r.*)
[698] This is in particular the case with provisions on the promotion of European works and commercial communications. The accessibility for persons with disabilities is safeguarded by the duty to offer at least 30% of the catalogue with relevant facilities.
[699] Broadcasting Act, op. cit.,, Article 18 paras 4-6, item 938.
[700] Ibid, Article 47a, item 913.
[701] Ibid, Article 47o, paragraph 1, p. 1 and paragraph 2, Article 47p, item 1019.
[702] This distinction is rooted in earlier texts of Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in member states concerning the pursuit of television broadcasting activities (Television without Frontiers Directive – TVWFD) and the AVMSD before it was amended by the Directive 2018/1808.

first category of content is completely prohibited in linear programme services and conditionally forbidden in VOD services – if made available without effective technical safeguards or other appropriate measures to prevent minors from accessing it.[703] Content falling within the second category may be broadcasted in programme services only between 11 p.m. and 6 a.m. and must be duly classified and marked regarding its potential to harm minors and the type of harmful content (violence, sex, vulgarisms, drugs);[704] in on-demand AVMS, such content is subject to the same classification and similar marking requirement.[705] Moreover, there is a duty to mark programmes broadcasted or made available on-demand, according to the degree of harmfulness to minors in different age groups. Categories of age groups are defined and described in the regulations by KRRiT; for linear programme services there are five categories (no age limit, from the age of 7, 12, 16 and 18), while for VOD services there are four age groups (no limit, from the age of 12, 16 and 18). In radio and television services, programmes labelled as suitable for minors from the age of 16 shall only be transmitted after 8 p.m.

With regard to VSP services, the Broadcasting Act refers to content that is "prejudicial to a healthy physical, mental or moral development of minors, in particular those containing pornographic content or exhibiting gratuitous violence". The transmission of such content without applying effective technical safeguards is prohibited. VSP providers have a duty to operate effective technical safeguards, including parental control systems or other appropriate measures, to protect minors from access to harmful content, and the duty to enable users to classify their uploaded content and apply technical safeguards. The conditions for classifying and marking content harmful to minors are set out in the KRRiT regulations, which distinguish four age categories: no age limit, 12+, 16+ and 18+. The regulation characterises them and establishes templates for visual indicators for content suitable for each of the three categories above 12 years of age.[706] As already mentioned, VSP providers are required to reflect these requirements on classification and marking, as well as the procedures for reporting content harmful to minors, in their terms and conditions.

[703] Such safeguards and measures are specified in the self-regulation: the Code of good practices of 26 June 2014, as amended in 2022, on detailed rules for the protection of minors in on-demand AVMS. These safeguards and measures include: a) a system – making the content available only after the provision of the data of a user's credit card, payment by credit card, electronic bank transfer or equivalent solution (e.g. PayPal), payment by adding to the bill, log-in to online banking system allowing age verification or confirmation of majority by an eID provider, and/or application of a technical system of effective parental control; b) another system making user access to content dependent on effective verification of majority (notified to IAB Polska). When applying one of these models, a provider may set a safe mode (parental protection) within a VOD service, removing inappropriate contents from view, disactivated only with a PIN code or equivalent measure to be administered by an adult user.

[704] Relevant graphic symbols have to be visible for TV viewers for at least five seconds before the broadcast and five seconds after each advertising break; radio broadcast are to be preceded with the specified verbal warning.

[705] However, the duration and placement of relevant graphic symbols is regulated more flexibly – with the requirement to allow a user of a VOD service to easily get to know the identification at the time of choosing the programme and during its duration.

[706] The regulation of KRRiT of 13 April 2022, Journal of Laws (*Dziennik Ustaw*) of 2022, item 1019.

6.2.3. Protection of minors in the context of access to pornographic content – new initiatives

The Polish Criminal Code[707] includes provisions addressing pornography, in particular penalising the public presentation of such content to individuals, who do not wish to be exposed, the dissemination of pornography accessible to minors under 15, and different provisionsconcerning pornography involving minors, animals or acts of violence.[708] However, the notion of pornography is not statutorily defined, but rather interpreted by legal doctrine and case law.

Recent concerns regarding the protection of minors against online harms, and in particular pornography, have led to legislative proposals aimed at restricting access for minors to such content. Available statistics highlight the scale of the problem: over 70% of children and adolescents declare that access to pornography is easy; the average age of first exposure is 11, while 18,5% of respondents declare having encountered sexual content before the age of 10. Moreover, 80% of children do not have parental control software on their mobile devices; about 54% of teenagers declare that their parents do not impose rules governing Internet use, while approximately 29% regard parental control of content and screen time as ineffective.[709]

Already in May 2023, the government presented a draft act on protecting minors from inappropriate online content,[710] allowing subscribers of internet access services to request from the providers of such services that they limit access to pornography. The proposal was withdrawn before the 2023 parliamentary elections. In early 2025, the Ministry of Digitalisation published the draft "Act on the protection of minors against access to harmful content online" (hereinafter the "ministerial draft") and launched public consultations.[711] A similar initiative, though limited to pornography, was submitted as a "citizens' draft" earlier to the *Sejm*.[712] The ministerial draft originally had a broad scope, as it covered pornography and other harmful content, without defining these notions. Following criticism during the consultations, a revised ministerial draft was narrowed to focus on pornography and accordingly renamed;[713] any references to other harmful content were removed. Nevertheless, those responsible for producing the drafts rejected calls to define pornography, claiming that the notion is sufficiently clear in criminal law doctrine

[707] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Act of 6 June 1997), consolidated text: Journal of Laws (*Dziennik Ustaw*) 2025, item 383.
[708] Polish Criminal Code, Article 202, paragraph 1, Article 200, paragraphs 3-6, Article 202, paragraphs 3-5.
[709] The statement of reason of the draft act by the Ministry of Digitalisation – 29 August 2025, 3, the file: *Projekt ustawy i uzasadnienie małoletni 29.08.2025 r.*.docx , pp. 13-14.
[710] *Sejm*, Governmental draft of 19 May 2023, (IX term) No. 3238.
[711] *Projekt ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w internecie* (Draft bill on protecting minors from access to harmful content on the Internet), showing the evolution of the draft act by the Ministry of Digitalisation with the statement of reasons and impact assessment, as well as contributions in consultations.
[712] Citizens' draft of the act on protection of minors against pornographic contents online and amending the act – Telecommunication Law. The draft was submitted on 20 December 2024 by a committee formed by certain conservative and pro-life organisations. The Constitution (Article 118.2) grants legislative initiative ability to a group of at least 100 000 citizens.
[713] The draft act on the protection of minors against access to pornographic contents online, 29 August 2025, made available on 1 September 2025.

and case law, and that a statutory definition might hinder a dynamic approach. Interestingly, the citizens' draft submitted to the parliament included a definition of pornography,[714] based on the elements of the notion of "sexually explicit content" as described in the Explanatory Report to the CoE Convention on Cybercrime.[715]

The ministerial draft proposes a mechanism to protect minors consisting of three main elements: 1) a requirement for providers of online services[716] offering access to pornography to implement effective age verification measures to prevent minors from accessing such content; 2) the establishment of a register of domain names of non-compliant services; 3) a duty for Internet access service providers to prevent access to websites using domain names listed in the register.

The obligation to implement effective age verification measures would apply to all providers of services provided by electronic means, which is the term used in Polish law as equivalent to "providers of information society services" in EU law. During consultations, some contributions proposed narrowing the draft's scope, e.g. to large-scale pornographic services, or to websites with a significant portion of pornographic content, or by exempting certain providers such as mere conduits or microenterprises. These suggestions were rejected by the drafters on the basis that differentiating obligations by provider type would lead to the unequal protection of minors.

The proposed rules are intended to have a broad territorial scope, applying to "providers providing online services to recipients within the territory of Poland, regardless of the provider's place of business or professional activity". Despite the argument, raised in consultations, of the country of origin principle under Article 3 of the eCommerce Directive, the draft does not include, with regard to providers based in the EU/EEA, any reference to requirements for measures derogating from this principle.[717] The statement of reasons for the draft explains that, in the interest of effectiveness, it is essential to allow actions against web pages originating from outside Poland, which are accessed by Polish minors, and refers to the "similar construction" of the DSA as applicable to intermediary services offered to recipients in the EU, irrespective of where the service provider is established.

The age verification mechanism is intended to establish unequivocally that the recipient of the service has reached the age of majority; self-declaration, age estimation methods and biometric methods are explicitly excluded. While the draft does not specify the exact methods to be used, it sets out the requirements for the mechanism, such as: ensuring the highest standard of protection of the personal data and privacy of the recipient; offering at least two methods that are universally accessible and easy to use for

[714] Article 2, p. 3 of the citizens' draft: "Pornographic content - content presenting, in any visual form, real, simulated, created and/or processed: a) sexual intercourse, including genital-genital, oral-genital, anal-genital or oral-anal, between persons of the opposite or same sex; b) masturbation; c) bestiality; d) portrayal of sadistic or masochistic practices in a sexual context."

[715] Explanatory Report to the Council of Europe Convention on Cybercrime, Paragraph 100. The Ministry of Digitalisation takes note of the Council of Europe's definition, but finds it insufficient due to the lack of the requirement for "the purpose to cause sexual arousal", which, according to the prevailing view, is an essential aspect of the notion of pornography under Polish criminal law.

[716] The draft refers to the notion of service provider in the meaning of Article 2, paragraph 6, UŚUDE – which is an equivalent of the notion of a provider of information society service under the eCommerce Directive.

[717] eCommerce Directive, Article 3, paragraphs 4 and 5; UŚUDE, op. cit.Article 3b.

recipients (including at least one suitable for persons with disabilities and/or non-Polish speakers); continuous availability of the chosen method; reliability of the data on which the method is based; prevention of easy circumvention of the method by users; and, where possible, interoperability of at least one method offered with other online services. Moreover, age verification must meet the criteria corresponding to a high assurance level for electronic identification means[718] and, if personal data processing is required, it must comply with the GDPR,[719] particularly the data minimisation principle; data collected may only be used for age verification purposes and must not be used for profiling recipients. Some of these data protection safeguards were introduced in response to concerns expressed in the consultations on the first ministerial draft. The statement of reasons for the draft refers to work on the EU Digital Identity Wallet, stressing that it will offer the possibility of age verification without providing additional information.[720]

The register of domain names offering access to pornographic content without prior age verification is to be managed by the Scientific and Academic Computer Network – National Research Institute (*Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy*) – NASK.[721] The selection of NASK is based on its experience and technological background; notably, its existing role in maintaining the dangerous websites warning list.[722] Before issuing the notification, the President of the UKE must inform the domain subscriber (service provider), allowing them two days to submit comments. The notification must also be communicated to the service provider, who may at any time object to the listing.[723] Objections are to be reviewed by the President of the UKE within 14 days, with the right to lodge a court complaint in the event of rejection. If the objection is upheld, the president must instruct NASK to remove the domain from the register within three days. Internet access service providers are obliged to prevent access to websites using domain names listed in the register, free of charge and within 48 hours of their register entry. Blocking is to be implemented by removing the relevant names from Domain Name Systems (DNS) and redirecting users to a UKE website displaying a specified message. If a domain is removed from the register, access must be restored within 48 hours. The register, maintained in an IT system to enable automatic date transfer to providers, will not be publicly available.

The ministerial draft also grants the President of the UKE powers to monitor the compliance of online service providers and Internet access providers with the above-mentioned duties, as well as to impose financial penalties, issue post-control

[718] As set out in Article 8(2)(c) of Regulation (EU) 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC [2014] OJ L 257/73.

[719] European Parliament and EU Council, Regulation (EU) 2016/679 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)

[720] For more information on the EU Digital Identity Wallet, see the dedicated website of the European Commission.

[721] Research and development organisation, data networks operator, and internet domain name registry operator for the .pl country-level top-level domain and a part of the national cybersecurity system.

[722] On the basis of the Act of 28 July 2023, on the fight against abuses in electronic communication, (*Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej)*, consolidated text: Journal of Laws (*Dziennik Ustaw*), 2024, item 1803.

[723] The lack of a deadline for filing the objection differs from the solution concerning listed gambling games, where a two-month limitation exists.

recommendations and adopt decisions ordering the removal of irregularities and specifying corrective measures. Unlike the citizens' draft and the Act on gambling games, which provide for restrictions regarding listed domains which are non-compliant with rules on the protection of minors, the ministerial draft does not propose prohibiting the provision of payment services on webpages listed in the register of domain names offering access to pornographic content without prior age verification.

As at late 2025, the draft ministerial act on the protection of minors against pornographic content online remains at an early stage of development. It is uncertain whether, when and in what shape the draft will be enacted. There is however no doubt, that the adoption of the law implementing the DSA would facilitate further consideration of additional initiatives regarding the protection of minors. The relationship of such initiatives with EU pieces of legislation, namely the DSA, the eCommerce Directive and the AVMSD, and provisions of Polish law implementing them and developing national public policy in respective areas remain a complex matter, requiring further careful consideration.

6.3. The example of the UK

Dr Mariette Jones, Senior Lecturer in Law, Middlesex University, London

6.3.1. National legal framework concerning platforms in the Online Safety Act

Almost a decade in the making, the Online Safety Act (OSA) of the United Kingdom became law in September 2023;[724] since then it has seen most of its provisions become applicable and is expected to be fully operational by 2026. The OSA is huge, both in size and number of regulations, as well as in its scope and stated aims. It attempts to address almost the entirety of possible harms that can be perpetrated online or via an online medium, and with regards to children, it does not restrict itself to illegal content but also regulates "legal but harmful" online content.

The OSA's core operational feature entails the state compelling private companies to actively monitor, evaluate, and remove content created by third parties and mandates measures aimed at protecting children such as enhanced age verification. For example, since 25 July 2025, services which publish pornographic content must use "highly effective age assurance" to prevent children from accessing it.[725]

[724] UK Government, Online Safety Act 2023.

[725] Section 81 of the OSA mandates:

(2) A duty to ensure, by the use of age verification or age estimation (or both), that children are not normally able to encounter content that is regulated provider pornographic content in relation to the service. (3) The age verification or age estimation must be of such a kind, and used in such a way, that it is highly effective at correctly determining whether or not a particular user is a child.

The OSA applies to a wide range of user-to-user services, search engines and content providers that are accessible to UK users, regardless of where the service is based. It covers both "user-to-user services", including platforms where users can upload and share content, such as YouTube or Facebook, as well as "search services" which include search engines such as Google. A user-to-user service is a regulated service if it has a substantial number of users in the UK. With limited prescribed exceptions (such as emails and messaging services), all user-generated content on a regulated user-to-user service is itself regulated.

The OSA applies additional duties to various categories of services. The most intensive duties and oversight apply to "Category 1" services. When the OSA was first introduced, it had separate provisions that were designed to protect adults from "legal but harmful" content. Although those provisions were removed, they were replaced by the duties that apply to Category 1 providers. Category 1 providers are those which on average have more than 34 million monthly UK users, and which use a content recommender system, or one that has more than 7 million monthly UK users, uses a content recommender system, and provides a functionality for users to forward or share regulated user-generated content on the service with other users of that service.[726] Services likely to be accessed by children have additional, more onerous obligations.

The OSA identifies the following main categories of harmful content: first, there is illegal content such as terrorism, child sexual exploitation and abuse, hate speech and fraud. Then there is content harmful to children, which is subdivided into primary priority content (e.g. pornography or content promoting suicide, self-harm or eating disorders), priority content (e.g. bullying, incitement to hatred or to participate in dangerous stunts) and non-designated content that nevertheless poses a material risk of significant harm.

The regime enacted is not the usual "notice-and-takedown" system familiar from other legislation and jurisdictions, but instead a proactive requirement to identify and remove certain content. The OSA imposes duties on all regulated user-to-user services. These include duties to assess, mitigate, and manage risks posed by certain types of illegal content, enabling users to report illegal content, the provision of a complaints procedure and duties to have regard to freedom of expression and privacy when implementing safety measures and policies.

As mentioned, Category 1 providers have more onerous duties, namely to (1) give users a choice about whether to verify their identity and the type of content they see, including whether they see content from users who have not verified their identity; (2) protect free speech; (3) protect users from fraudulent advertising; (4) ensure compliance with the service's terms (including that the service provider takes down user-generated content if, but only if, that content does not comply with the terms of service; (5) publish an annual "transparency report" to Ofcom[727] (see below 6.1.3.4) containing such information as Ofcom requires; and (6) miscellaneous additional duties, including to summarise the service's most recent illegal content risk assessment and children's risk assessment and to make provision for a complaints procedure.

[726] Regulation 3 of the OSA (Category 1, Category 2A and Category 2B Threshold Conditions) Regulations 2025.
[727] Ofcom (Office of Communications) is the regulator for communications services in the UK.

In short, the OSA imposes a duty of care analogous to the duty of care in tort/delict or health and safety laws. Platforms must now take measures to prevent illegal content from being posted, and where it has been posted, remove or disable access to it. This includes content that is already well-established as being illegal in UK law, such as terrorism-related content, child sexual abuse material, hate crimes, fraud and so forth. Regarding children, this duty extends to otherwise legal content that may be harmful to children (see below 6.3.2). In addition to this content moderation duty, service providers and platforms also have a duty to undertake risk assessments and to put in place appropriate mitigation, as well as reporting and platform design duties.

To enforce the newly created duties, the OSA confers extensive new powers on the independent body Ofcom which is the statutory regulatory body supervising the communications industry in the UK. It designates Ofcom as the independent online safety regulator. Its role includes overseeing and enforcing the new regulatory regime.[728]

In order to do this, Ofcom is responsible for drafting codes of practice to flesh out the OSA's provisions. Codes include, *inter alia*, guidance on: platform design choices, recommendation algorithms, content moderation, oversight and governance, complaints and reporting tools and parental controls, assessing compliance and investigating breaches, enforcing duties and imposing sanctions.[729] These are potentially vast, with fines of up to GBP 18 million or 10% of worldwide turnover as well as blocking services being possible.[730]

6.3.2. Specific rules for the protection of children

Children are recognised as particularly vulnerable online users who are more susceptible to exploitation, manipulation, and psychological harm. The OSA therefore aims to provide enhanced online protection to children,[731] by adopting a "safety-by-design"[732] philosophy which requires platforms to proactively protect persons under 18 years of age.[733] The OSA mandates platforms likely to be accessed by children to implement child safety risk assessments and to take pre-emptive steps to prevent harm.[734] Section 37 of the OSA casts the net very wide, by effectively defining the term "likely to be accessed by children" as any instance where "it is possible for children to access the service or a part of it".

The duty to prevent harm includes protection from not only illegal content such as sexual abuse material, but also legal content that may be harmful, such as content promoting or resulting in self-harm, suicide or eating disorders, and pornography.[735] Steps

[728] UK Government, Online Safety Act 2023, part 7.
[729] UK Government, Department for Science, Innovation and Technology, Online Safety Act: Protection of Children Codes of Practice – explanatory memorandum – GOV.UK, 24 April 2025.
[730] Schedule 13 of the OSA; OSA (Qualifying Worldwide Revenue) Regulations 2025/1032.
[731] Ibid., Section 1(3)(b)(i).
[732] Ibid., Section 1(3)(a).
[733] These duties are introduced in Sections 11 "Children's risk assessment duties", 12 "Safety duties protecting children", and 13 "Safety duties protecting children: interpretation" of the OSA, op. cit.
[734] Ibid., Sections 35, 36 and 37.
[735] Ibid., Section 61.

to take include strict age assurance measures through the use of appropriate verification technologies, setting algorithms in such a way as to prevent harmful content being recommended to minors and considering children when setting permission features for group chats or being added automatically, and preventing unwanted contact such as children receiving direct messages from strangers.[736]

For age verification the OSA requires more than just self-reporting: methods such as facial recognition or ID checks must be used.[737] It is likely that it will prove difficult to balance this duty with competing privacy and data protection laws that are also, in their turn, more protective of children than adults. Governance requirements include appointing senior personnel responsible for compliance. Clear reporting channels should be published, as well as the platform's content policies and what technologies are used to detect harms. Transparent complaints and reporting systems must be made accessible to minors and their guardians. The OSA further holds platforms accountable by requiring them to conduct regular children's risk assessments and to post summaries of these publicly.[738]

6.3.3. Online gambling, children, and the Online Safety Act

The OSA created new offences, such as "cyberflashing",[739] and brings under one umbrella existing criminal law provisions as far as they occur or are facilitated online. In addition, one of the most significant aspects of the OSA is the imposition of legal duties concerning content that is legal, but which may be harmful to children, as set out above. The admixture of existing legal provisions and criminal offences, and the way in which the act extends and extrapolates from there regarding children is illustrated by its effect on the UK's legal regime concerning gambling.

The Gambling Act 2005[740] is the principal law concerning gambling in the UK. One of its three licensing objectives is to protect children and other vulnerable persons from being harmed or exploited by gambling. The Gambling Act makes it an offence to invite, cause or permit anyone under the age of 18 to gamble, and it provides for an age verification and licensing regime that ensures that only persons over 18 can gamble online, with the onus on licenced operators to verify identity and age. Advertising of gambling is regulated via rules made by an independent body: the Advertising Standard Authority (ASA)'s Committee of Advertising Practice (CAP). The rules set by CAP as well as regulations under the Gambling Act and the Gambling (licensing and advertising) Act 2014[741] prohibit advertisements targeted at or which strongly appeal to minors, and provide that people who appear under 25 years of age should not be featured in most gambling advertisements.

[736] Ibid., Sections 11, 12, and 13, as well as the corresponding duties placed on search engines in Sections 28, 29 and 30.
[737] Ofcom, Age Assurance and Children's Access Statement, 16 January 2025.
[738] Section 36 OSA.
[739] Crown Prosecution Service, "Prison sentence in first cyberflashing case", 19 March 2024.
[740] UK Government, Gambling Act 2005.
[741] UK Government, Gambling (Licensing and Advertising) Act 2014.

The way in which the OSA complements existing UK legislation is showcased well in this area. It enhances the existing protection of minors by extending responsibilities and mandates to platforms that host or promote gambling content. For instance, the Gambling Act's provisions prohibiting underage gambling, and requiring licenced gambling operators to verify age, now extend to social media platforms, search engines, and streaming platforms. Tasked with applying the advertising codes[742] under the Gambling Act, the ASA in 2023 banned several gambling advertisements that used animation and cartoons that were likely to appeal to children.[743] These were assessed as being in breach of section 16 of the Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code),[744] which states that marketers should not exploit the young or vulnerable. The ASA also banned advertisements featuring top footballers promoting gambling platforms, as these were found to be particularly attractive to minors.[745] Therefore, whereas existing legislation operated in a reactive fashion, such as by assessing advertisements as set out above, the OSA coming into effect now means that henceforth these entities must take proactive measures to prevent children from being exposed to gambling advertisements and content promoting gambling.

Furthermore, whereas up to now potential liability for the promotion of gambling websites lay primarily with the websites themselves, or with their promotors such as influencers on platforms like YouTube, the OSA in effect extends potential liability to the platforms themselves which host the websites, influencers and promotors.

Another illustrative point relates to activities in online games which mimic gambling mechanics by encouraging children to spend money on chance-based rewards, such as the inclusion of loot boxes in online games. These contain randomised items in which the player does not know what they are going to get until they have opened the loot box. Players can typically buy loot boxes with money (including via virtual currencies) or access them via gameplay. Concerns have been raised that these mechanisms in games may be harmful to children – they may, for example, foment gambling addiction.[746] The Gambling Act 2005 does not regulate loot boxes as gambling, and after extensive consultation the UK government declined to legislate against loot boxes, instead calling for self-regulation by the industry to minimise risks in 2023.[747] It is significant, however, that it recognised concerns by, amongst others, the UK Gambling Commission about the potential risks to children and vulnerable players. By mandating a proactive duty to prevent

[742] Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code); Code of Broadcast Advertising (BCAP Code).
[743] See for instance, ASA, "ASA Ruling on Buzz Group Ltd.", Complaint Ref. A23-1217474 Buzz Group Ltd, Press Release, 3 January 2024.
[744] Code of Non-broadcast Advertising and Direct and Promotional Marketing (CAP Code).
[745] For particular cases, see ASA, "Gambling, betting and gaming: Appeal to children – ASA | CAP", 9 May 2023. As well as ASA, "ASA Ruling on LC International Ltd t/a Ladbrokes", Complaint Ref. A22-1171467 Ladbrokes Betting Gaming Ltd, Press Release, 21 December 2022.
[746] Zendle, D. et. al. (2020) "Paying for loot boxes is linked to problem gambling, regardless of specific features like cash-out and pay-to-win", *Computers in Human Behavior,* 102, pp. 181-191, cited with approval of the UK Government, Department for Culture, Media and Sport: Government response to the call for evidence on loot boxes in video games – GOV.UK, 18 July 2022.
[747] UK government Department for Culture, Media and Sport Loot boxes in video games: update on improvements to industry-led protections – GOV.UK, 18 July 2023.

legal but potentially harmful content to children, the OSA has now transformed industry self-regulation into legal regulation.

Considering all of the elements discussed above, the OSA is ambitious in scope, aims and operation, and as such presents challenges on a variety of fronts. To name but one instance, the "highly effective" age assurance mandate which could include biometric or documentary verification may infringe privacy and data protection provisions and raises questions about inclusivity for children without formal ID, not to mention issues around the technical feasibility of implementing robust but non-invasive verification systems, especially for smaller service providers.

Ofcom, as the competent regulatory authority, as well as those regulated by the OSA, face burdensome and exacting duties that are in many aspects not yet fully clear. These duties will only become clear after having been tested in the courts and willlikely have to be addressed in further regulation or codes of practice. Wikipedia recently launched the first legal test of the new regime when it objected to the way in which Ofcom defined Category 1 services in Regulation 3 of the OSA.[748] It challenged, the fact that, as a charitable, non-profit organisation, it was being put in the same category as massive multinational corporations such as Google or Facebook. In its August 2025 judgment, the High Court of England and Wales allowed judicial review of two aspects of Ofcom's decision-making process but decisively disallowed Wikipedia's two human rights-based challenges.[749] The case may still be appealed, and it is fully expected that the legislation and related regulations will be further tested in the courts, as it may prove to significantly impact areas of law such as freedom of speech and privacy, as well as the UK's digital and wider economy.

[748] *Wikimedia Foundation (a charitable foundation registered in the United States of America), BLN v. Secretary of State for Science, Innovation and Technology* [2025] EWHC 2086 (Admin).
[749] Ibid., paragraphs 133-137.

7. Comparative analysis

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg, and Dr Sandra Schmitz-Berndt, Research Associate, Institute of European Media Law (EMR)

Despite a shared international fundamental rights framework and, in most of the countries covered in this publication, a joint EU legal framework, the national reports reveal variations in how law enforcement is applied to Internet intermediaries across Europe.

A full understanding of the challenges of enforcing the applicable laws against illegal content and disinformation in Europe requires comparing national legal requirements as well as sanctions mechanisms and country-specific solutions in this regard. Although EU legislation – mainly through the recent additions to the "digital rulebook" – has driven substantial harmonisation directly binding only for its member states, third countries like Türkiye are also seeking to align their laws with EU standards.

With a focus on enforcement, the following analysis will not address national differences about what is understood as illegal content, in particular not in national criminal law. A true "Europeanisation" of criminal law has not yet taken shape beyond the EU's jurisdiction, and within the EU harmonisation is so far restricted to particularly serious crimes with a cross-border dimension under the Lisbon Treaty and the implementation of police and judicial cooperation under the TFEU. Additionally, harmonisation in some instances concerns certain behaviours that endanger core EU values such as those targeted by the Directive on combatting violence against women and domestic violence.[750] In contrast it is especially interesting to observe differences in national approaches when dealing with content that might not be illegal per se, but which is regarded to have harmful effects, such as the currently much debated problem of how to respond to disinformation campaigns, which is why this area is the initial point of analysis below before taking a closer look at the national approaches to enforcing rules aimed at illegal content and, in the last section, other types of harmful content rules.

7.1. The enforcement of rules countering disinformation

Disinformation in the EU appeared as a serious challenge in connection to broad issues including information spread about health matters, "conspiracy theories" and foreign (political) influence. It is now addressed as a systemic risk in the online environment through a combination of voluntary and legal frameworks, particularly focusing on so-called FIMI campaigns and electoral interference. Therefore, the EU has progressively shifted from soft measures such as the 2018 Code of Practice on Disinformation to binding obligations under the DSA, thereby strengthening its disinformation response through a

[750] Directive (EU) 2024/1385, op. cit.

mix of self-regulation, enhanced coordination, and improved risk detection. This approach is further backed by the TTPAR and EMFA which address issues such as foreign-funded political ads and rogue media services. Recognising the critical role of VLOPSEs for accessing information, self-regulatory commitments are thus accompanied by increased due diligence obligations for providers of VLOPSEs. Countering disinformation with enforcement measures, the DSA relies on a hybrid enforcement system whereby the European Commission and EU member states act as co-regulators adding to the role of intermediaries themselves. National competent authorities are responsible for the oversight and enforcement of the DSA in areas not explicitly delegated to other appointed authorities, meaning that national authorities enforce rules in relation to providers of intermediary services established within their territory. The European Commission is primarily responsible for supervision and enforcement in relation to VLOPSEs. This two-tier enforcement approach is exemplified by the case of TikTok as analysed in the Romanian country report.

Romania, with its widespread reliance on platforms like Facebook, WhatsApp, YouTube, and TikTok as information sources – a trend comparable to developments in other member states – coupled with low levels of digital literacy, constitutes an environment that is particularly vulnerable to disinformation. As such, it has emerged that the population there was especially prone to disinformation campaigns having an impact on public opinion and democratic processes. That risk materialised ahead of the 2024 presidential elections, at a time when the DSA had already been fully applicable. The Romanian example indicates the limits of the DSA which focusses more on the introduction of mechanisms than a definitive set of rules to tackle and mitigate the systemic risk of disinformation and election interference. This gap has now been partly addressed through the Strengthened Code of Practice on Disinformation which was initially voluntary but has now been integrated into the framework of the DSA as the Code of Conduct on Disinformation. By its integration into the DSA framework in February 2025, the Code will serve as guidance for VLOPSEs to achieve compliance with their obligations with regard to systemic risks.

Romania, with its widespread reliance on platforms like Facebook, WhatsApp, YouTube, and TikTok as information sources – a trend comparable to developments in other member states – coupled with low levels of digital literacy, constitutes an environment that is particularly vulnerable to disinformation. As such, it has surfaced that the population there was especially prone to disinformation campaigns having an impact on public opinion and democratic processes. That risk materialised ahead of the 2024 presidential elections, at a time when the DSA had already been fully applicable. The Romanian example indicates the limits of the DSA which focusses more on the introduction of mechanisms than a definitive set of rules to tackle and mitigate the systemic risk of disinformation and election interference. This gap has now been partly addressed through the Strengthened Code of Practice on Disinformation which was initially voluntary but has now been integrated into the framework of the DSA as the Code of Conduct on Disinformation. By its integration into the DSA framework in February 2025, the Code will serve as guidance for VLOPSEs to achieve compliance with their obligations with regard to systemic risks.

In parallel to these proceedings at EU and national level, policy measures were adopted in preparation for the elections that were repeated after having been annulled due to external influence. These policy measures benefitted from the increased cooperation mechanisms

introduced by the different parts of the new EU digital legal framework. For instance, a round table with VLOPSEs, the Romanian Digital Services Coordinator (ANCOM), relevant state authorities and civil society organisations sought to gather information and ensure preparedness for the ongoing Romanian elections.[751] In view of the duration of the European Commission's formal proceedings, it was understandable that the national legislator sought to address the perceived shortcomings by national measures. However, in view of the CJEU's decision[752] concerning the Austrian Communication Platforms Act which was invalidated for disregarding the country-of-origin principle under the eCommerce Directive, it remains unclear whether a law such as the one that has been proposed (but not yet finally voted on) in Romania would be regarded as compatible with relevant EU secondary law. The Romanian proposal would, *inter alia*, require platforms to limit the spread of potentially harmful content to no more than 150 users, and remove illegal content within 15 minutes of publication based on automated classification.

The example of France in this context shows how national regulatory and policy measures can support the objective of fighting disinformation in tandem. In contrast to the Romanian draft bill, the French approach does not interfere with harmonised EU platform regulation but puts the national focus on fighting disinformation by means of a legal framework concerning the algorithmic identification of such material and thereby indirectly supporting DSA rules with an enforcement component. An important means of reaching the goal is the accompanying work of the dedicated body VIGINUM which monitors, detects and analyses FIMI, and, notably, identifies and characterises the techniques applied and the threat actors involved in order to increase preparedness and public awareness. In the absence of a formal mandate to enforce rules against false information, VIGINUM's role remains supportive. The French focus on awareness raising is also reflected in further actions such as improving information literacy at school level. France has given significant attention to finding responses to the risks of FIMI reflected not only in VIGINUM's tasks but also in the Léotard Law which, *inter alia*, mandates ARCOM to take action against audiovisual communication services which are controlled or influenced by a foreign state and which deliberately broadcast false information, in particular in the three months preceding an election.

While the overarching framework for France and Romania, as well as all other EU member states is mostly harmonised due to EU regulations in place, it is interesting to contrast this with a non-EU/EEA country which is party to the ECHR. In this context, Ukraine serves as a particularly vivid example since it has been exposed to massive FIMI campaigns by a hostile actor for more than a decade. Ukrainian legislation does not regulate online platforms but only VSPs under its jurisdiction with the Ukrainian Law on Media. Regarding platforms more generally only soft law approaches like memoranda or cooperation agreements are foreseen so far. This regulatory gap is perceived as concerning given Russia's large-scale information attacks and the growing reliance by the population on social media for news, which is at the same time used for the dissemination of disinformation. However, with the introduction of the martial law in 2022 that also

[751] European Commission, "Commission, Online Platforms and Civil Society Increase Monitoring During Romanian Elections", Press release, 5 December 2024.

[752] C-376/22 Google Ireland Ltd and others v. Kommunikationsbehörde Austria (KommAustria) [2023] ECLI:EU:C:2023:835.

facilitates restrictions on speech, temporary blockings of on-demand audiovisual media services and the services of audiovisual service providers of the aggressor state on the territory of Ukraine became possible. Further, VSPs are obliged to include temporary prohibitions on disseminating disinformation related to the armed aggression against Ukraine.

The lack of effective mechanisms for the state to influence foreign online platforms in order to protect its national interests resulted in the blocking of websites and online platforms on the basis of the Law of Ukraine on Sanctions and as a consequence of the Russian large-scale invasion of Ukraine also pursuant to specific orders from the National Centre for Operational and Technical Management of Telecommunication Networks. Without a dedicated framework on the conditions for these blocking measures, they remain controversial. The blocking of such services is also possible under the martial law. However, these measures are intrinsically linked to the protection of national interests and as such need to be seen as *ultima ratio* in view of the lack of a more general regulatory framework for online platforms. Similar to France, Ukraine also employs preventive control by seeking to increase media literacy and awareness-raising campaigns including on how to identify disinformation and in particular FIMI.

7.2. The enforcement of rules countering terrorist content

Responding to terrorist content online, the EU employs a combination of binding regulation and voluntary cooperation by the intermediaries, both introducing platform-specific duties in combination with combatting such content.

The AVMSD imposes an obligation on EU member states to ensure by appropriate means that AVMS providers and VSP providers under their jurisdiction do not contain any content which constitutes public provocation to commit terrorist offences.[753] In June 2022, the TCOR introduced a more broadly applicable set of harmonised rules covering all hosting service providers offering services in the EU. Besides a uniform definition of terrorist content, it introduced removal orders requiring providers to take down terrorist content within one hour, as well as voluntary removal requests; it notably also includes procedural rules in both regards. An emphasis is put on cross-border cooperation and coordination between member states and, for instance, also Europol. In addition, under the DSA, terrorist content constitutes a systemic risk which means that VLOPSEs have to conduct a preventive risk assessment concerning such content. This prescriptive regulation is complemented by voluntary cooperation and coordinated response mechanisms.

How the TCOR framework operates in practice is exemplified by the insights from Germany being the member state in which authorities were particularly active in taking steps to remove content under the TCOR following the Hamas terrorist attack on Israel. In fact, Germany emerged as the most proactive EU member state in enforcing the TCOR as well as – in this context – referring the largest number of cases under the DSA to the European Commission for further investigation. The German enforcement approach

[753] AVMSD, op. cit., Article 6.

regarding the TCOR benefitted from pre-existing institutional infrastructure and experience with a central reporting hub based on prior national legislation targeting the take down of illegal content. which – as a legal basis – has in the meanwhile widely been replaced by the harmonised provisions. The application of the TCOR in Germany has shown a compliance rate by intermediaries with removal orders of more than 95%. Instead of focusing on formal removal orders, Germany relies heavily on referrals requesting voluntary removal before removal orders are issued. The BKA acts as the central authority under the TCOR and is also competent under Article 18 DSA for notification of criminal content. The strict enforcement of the TCOR also reflects the historical sensitivity to terrorism and antisemitism, and ultimately the advanced legal and institutional readiness of the member state due to its earlier legislation and institutional structures that had been introduced on that basis.

An equally intensive stance against terrorist content online is taken by the non-EU member state Türkiye. However, besides the Turkish Internet Law requiring the removal of illegal content by the host provider, if content is not removed voluntarily, the long-standing practice of administrative authorities in Türkiye was to block access to entire websites, which has raised serious concerns for freedom of expression and media as also illustrated by judgments of the ECtHR in such cases coming from Türkiye. The effectiveness of this approach is also questionable, as content remains available outside the restricted territory. Accordingly, Türkiye's new regulatory approach targets the removal of unlawful content at its source, rather than merely restricting access. For terrorist content a short time frame of four hours for removal applies. Social media platforms must appoint local representatives, respond to user requests, issue transparency reports, localise data, and protect minors in ways that are similar to the DSA's regulatory regime. To enforce compliance, Türkiye has introduced sanctions including fines, advertising bans, bandwidth throttling, and shared liability for illegal content. In practice, it seems that access blocking, in particular in times of civil protests, is still heavily used for various reasons.[754]

7.3. The enforcement of rules countering defamatory, hateful and violence-inciting speech

The EU's regulatory approach to defamatory, hateful and violence-inciting speech online has evolved in response to the rise of such speech, particularly in digital spaces. While the 2008 Council Framework Decision on Racism and Xenophobia provides a baseline definition of illegal hate speech, member states often extend protections against hatred based on other grounds than the ones included in the framework decision's definition, such as gender or disability.

As mentioned previously, the DSA introduced layered responsibilities for online platforms with a number of obligations specifically for VLOPSEs. The Code of Conduct on Countering Illegal Hate Speech Online, revised as the Code of Conduct+ in 2025, has been integrated into the DSA's co-regulatory framework. It supports faster removal of illegal hate

[754] See e.g. Schräer F., "Access to Various Internet Platforms in Turkey Restricted", heise.de, 20 May 2025.

speech and aligns platform moderation. The EU has begun enforcing these rules against VLOPSEs for which the Commission has competence. Notably, the Commission took action against X (formerly Twitter), citing inadequate risk mitigation and moderation practices. The European Commission invoked investigatory powers under the DSA and continues to monitor compliance.[755]

Challenges persist, especially around content like defamation, where legality depends to a large extent on context and national standards. As the country examples show, some differences exist as regards the national criminal and civil law rules that apply to defamatory, hateful or violence-inciting speech albeit these rules being subject to the same European and international human rights standards. Compared to Ireland, for example, Italy has clearer criminal liability tied to defamatory or hate content via public communication means. The example of Ireland in turn proves that laws that have proven effective in the offline world, are possibly not applied to online speech with the same effectiveness.

As regards liability, the DSA maintains the eCommerce Directive's principle of no general monitoring obligations for intermediaries, but allows for injunctions that can require platforms to prevent the reappearance of illegal content similar to what has already been established previously as illegal (i.e. "staydown" obligations), as long as the consideration of such an injunction does not require independent legal assessment to be undertaken by the providers concerned.

Increased EU harmonisation in the form of a directly applicable regulation (DSA) rather than a Directive (eCommerce Directive), which is only binding as to the goal, but requires national transposition, means that there is an overarching uniform platform regulatory framework across the EU country examples included in this publication. However, as the examples show, the actual enforcement relies on national mechanisms. In comparison to Ireland, Italy has a more advanced regime of enforcement in practice with strong administrative powers vested in the national regulatory authority for communications AGCOM, which is also the DSC under the DSA. Italy's system – combining EU-aligned rules (DSA, AVMSD), national instruments (TUSMA, Mancino Law), AGCOM's administrative role, and court remedies – forms a layered enforcement structure. In contrast, much of the platform liability in Ireland used to be built around civil liability and notice, with limited past regulation (pre-DSA) specifically targeted at the obligations of platforms with regard to hate speech and defamation. It seems that a delayed transposition of parts of the revised AVMSD and the new Irish supervisory authority CnAM which was only established in March 2023 meant that until now, as a consequence of this delay, there has been limited enforcement action, despite CnAM also being responsible for enforcing the DSA nationally and being the Online Safety Regulator. However, with the European Commission's exclusive powers to supervise systemic risks of VLOPSEs and recent actions taken by the Commission in that regard, increased activities can be seen and further expected from CnAM, *inter alia*, in supporting the European Commission's work by gathering and sharing information about the many Irish-based VLOPSEs.

[755] See also now the first DSA-based sanction decision concerning a part of the investigation against X not relating to the elements discussed here, European Commission, "Commission fines X €120 million under the Digital Services Act", Press release, 5 December 2025.

While increased enforcement action ensures that rules and obligations are effectively applied and implemented, the example of Austria emphasised another aspect of combatting online hate. The example showed that, given the full harmonisation of liability rules applicable to intermediary services at EU level, the scope for regulating illegal online content is largely confined to substantive law. The new Austrian legislation on hate on the Internet was introduced in response to emerging forms of online hate seeking to better reflect the specific characteristics of communication in cyberspace. Amendments to the existing domestic framework countering defamatory, hateful and violence-inciting speech also address procedural law and thereby facilitate and support private enforcement.

7.4. The enforcement of rules targeting other areas of harmful content

Shifting from discussing the removal of illegal content, the final focus area of this IRIS Report is other harmful but lawful content. Said content particularly includes material unsuitable for children which can impair the development of minors, such as pornography. Within the EU, the AVMSD, which applies both to traditional broadcasting and to on-demand services, as well as in parts – including the obligation to protect minors – to VSP providers, requires EU member states to ensure such content is inaccessible to minors through tools like age verification and classification systems applied by the providers. The DSA complements this by imposing horizontal obligations on online platforms, requiring them to take appropriate and proportionate measures to protect minors, including privacy and safety-by-design standards. In July 2025, the European Commission issued guidelines under Article 28 DSA recommending measures such as age assurance tools, emphasising proportionality, children's rights, and minimal data disclosure – potentially to be realised by using the upcoming EU Digital Identity Wallet. Enforcement has already begun in this context with the Commission having initiated proceedings against major pornography platforms in 2025 for insufficient age verification, while national authorities coordinated parallel actions through the EBDS ensuring an alignment of enforcement action against such content.

The example of Poland indicates that some member states are struggling with domestic DSA implementation[756] and thus failing to provide for national enforcement procedures. In September 2025, the Polish Government finally adopted the national implementing act which will significantly revise the existing legal framework. As an EU member state, Poland follows the previously described DSA and AVMSD decentralised enforcement model with special competences as regards VLOPSEs assigned to the European Commission. While the draft act implementing the DSA details procedures for the removal of illegal content, it does not specifically address legal yet harmful content beyond the directly applicable rules of the DSA. However, specific rules on harmful content can be

[756] In May 2025, the European Commission decided to refer several member states including Poland to the CJEU for failure to designate and/or empower a national DSC under the DSA, see European Commission, "Commission Decides to Refer Czechia, Spain, Cyprus, Poland and Portugal to the Court of Justice of the European Union due to lack of effective implementation of the Digital Services Act", Press release, 7 May 2025.

found in *leges speciales* dealing for instance with online gambling or VSPs. In practice, limiting access to, for instance, pornography on VSPs does not hinder the accessibility by minors when such content can be easily accessed online elsewhere. The Polish legislator seeks to close this regulatory gap by introducing a new act on the protection of minors against access to harmful content online. The draft act primarily focuses on preventing access to pornography by minors by requiring online services to implement effective age verification measures comparable to those required for VSPs under the national implementation of the AVMSD.

Similar to the existing online gambling regulation, the rules on access restrictions are accompanied by a detailed enforcement regime. In both instances, Poland employs a register-based enforcement model combining administrative designation (listing of non-compliant sites) with technical obligations for intermediaries. Accordingly, enforcement is not directly addressed at the non-compliant services which are regularly located outside the territorial jurisdiction of Poland. The gambling framework adds a financial enforcement dimension with blocking of payments to non-compliant services, whereas the draft Act on the protection of minors against access to harmful content online focuses purely on content access control. This distinction reflects the differing economic structures and regulatory purposes of the two regimes. Online gambling services derive their revenue from direct user payments, hence, prohibiting payment services is an effective enforcement tool that cuts off the operator's income stream and protects consumers from financial loss. Moreover, the enforcement model hinders a monetary exchange between underage users and operators. In contrast, most pornography websites operate an advertising-based or traffic-monetisation model, offering free access to users and earning revenue from third-party advertisers or affiliate networks. The draft act reflects the limited practical effect of blocking payments in this constellation and thus focuses on access prevention as a more targeted and proportionate measure aligned with its protective objective.

In contrast to regulation of harmful content in the EU, which is encompassed in different specific legal acts, the UK seeks to provide for an all-encompassing legislation. Following Brexit, the UK adopted the OSA as a domestic UK statute that sets out a substantive national regime that regulates both illegal and harmful online content. The OSA goes significantly beyond the DSA in both scope and depth of regulation, creating new legal duties on platforms. Enforcement under the OSA is centralised under a single national authority, Ofcom, the UK's communications regulator that is vested with extensive investigatory, supervisory and sanctioning powers, including fines of up to 10% of global turnover or service blocking.

Under the OSA, platforms are faced with mandatory proactive duties of care requiring them to identify, remove and prevent illegal and harmful content for minors. In effect, liability is shifted toward platforms in a much greater effort than under the DSA. In summary, the DSA imposes, *inter alia*, systemic risk assessment, transparency reporting and notice and action mechanisms, but Article 28 DSA, for example, only requires platforms accessible to minors to take appropriate and proportionate measures to protect them, while remaining risk-based and flexible. The OSA's child protection provisions in contrast mandate strict age assurance measures, "safety-by-design" systems and regular risk assessments, extending to sectors like online gambling and gaming loot boxes. Enforcement has already led to regulatory actions and legal challenges – such as

Wikipedia's judicial review against Ofcom – highlighting tensions between online safety, privacy, and freedom of expression as the regime moves toward full implementation by 2026.

8. Conclusions and looking ahead

Dr Mark D. Cole, Director for Academic Affairs, Institute of European Media Law (EMR) and Professor in Media and Telecommunication Law, University of Luxembourg

The digital environment has redefined both the reach of expression and the scope of responsibility in the context of expressed information and disseminated information. As this IRIS Report demonstrates, the same online infrastructure that enables unprecedented participation and pluralism in public discourse also magnifies the risks posed by illegal content and disinformation to individual rights, social cohesion, and democratic resilience. The online environment is at the same time dominated by a small number of powerful platforms. Legal frameworks at international, but moreover at European, and national levels have gradually evolved to address these risks, yet enforcement remains in parts fragmented and uneven, reflecting variations in national traditions, regulatory capacities, and political priorities. The DSA, as well as the OSA in the UK, and other emerging instruments signal a shift towards more systematic, risk-based and proactive regulation of online intermediaries, but they also expose the persistent tension in enforcement measures between protecting freedom of expression and ensuring online safety and accountability.

Effective enforcement cannot be achieved through purely national action or unilateral measures. The borderless nature of online communication requires cross-border cooperation and mechanisms that foster consistency while respecting national legal orders and fundamental rights guarantees. It also requires greater transparency and procedural measures by platforms that increasingly function as gatekeepers in the digital sphere. Accordingly, the common thread of digital laws that has emerged recently is a focus on transparency and a risk-based approach to respond to and mitigate risks.[757] Enforcement thus evolves from ad hoc removal practices toward a coherent governance model.

Across all thematic areas examined in this report, three overarching dynamics can be identified:

First, enforcement models are diversifying in response to the differentiated roles and capacities of intermediaries. The initial liability privilege and "no general monitoring" principles inherited from the early web remain in principle, but they coexist with increasingly granular duties for platforms that play a systemic role in shaping public communication and thereby de facto question whether the safe harbour approach for intermediaries can sustain over time. The EU's risk-based regulatory approach, especially under the DSA but also under other legal interventions such as the TCOR, illustrates a shift from reactive, notice-and-takedown logic to forward-looking oversight. National examples show how member states implement common rules through (sometimes) distinct institutional and procedural rules. Non-EU countries such as Türkiye and Ukraine likewise

[757] See on this already Cappello M. (ed.), *Algorithmic transparency and accountability of digital services*, IRIS *Special*, European Audiovisual Observatory, Strasbourg, 2023.

demonstrate that domestic enforcement models are strongly shaped by political context, geopolitical realities and constitutional constraints.

Second, the limits of existing frameworks become most visible in relation to disinformation and other forms of harmful but lawful content. While illegality can, in principle, be defined, harmful content sits at the intersection of public interest, democratic security, and fundamental rights. For this category, regulatory intervention is inherently more contested and only the application of existing approaches will show in the future whether or not this area will also receive more strict regulatory attention.

Third, the national case studies highlight the growing importance of institutional capacity, cross-border cooperation and technical expertise. Legal rules alone do not ensure effective enforcement. Rather, outcomes depend on the maturity of regulatory authorities, the quality of inter-agency cooperation, access to technical tools and the engagement of platforms themselves as well as cooperation with them. The examples of Romania and Ukraine underscore the structural vulnerabilities of states with lower levels of digital literacy, greater exposure to FIMI, or limited leverage over global platform companies. Conversely, the experiences of Germany and France show how established regulatory infrastructures can provide for rapid and coordinated responses — though even these systems must continuously adapt to new risks and technologies.

The selected examples of disinformation, illegal and harmful content indicate that there is no one-size-fits-all approach, but regulation may require measures proportionate to the risks that stem from the content. Similar to the granular approach in the DSA with stricter rules for VLOPSEs and its general risk-based approach that can also be found in other technology regulation, such as the AI Act, some unwanted content may require stricter regulation with set time frames and harmonised procedures, as is the case in the EU regarding terrorist content, than other illegal content. The reported country examples on disinformation have shown that addressing disinformation demands more than punitive or takedown-based approaches. It calls for a more holistic societal response that includes strengthening media literacy and reliable media and ensuring that algorithmic design choices do not inadvertently amplify harmful narratives. Enforcement should thus not only deter harmful conduct but also reinforce the structural conditions that sustain trustworthy, pluralistic, and democratic information ecosystems.

Looking ahead, the protection of fundamental rights online – particularly freedom of expression, access to information and the right to participate in public debate – must remain the guiding compass for policymakers, regulators, and eventually platforms. At the same time, duties of states in safeguarding a situation where the opinion-forming process can take place in an independent, free and safe manner, as well as the EU's commitment to its fundamental values, may necessitate further regulatory action. Nonetheless, careful scrutiny of such rules is important to ensure that online enforcement does not lead to prematurely curtailing speech while being effective where necessary to respond to illegal and, under certain conditions, harmful speech. This need will only be further enhanced by the increasing impact that AI-driven "content" creation has on the communication sector, including the market impact of diverting attention and refinancing means away from the sources that created the information content initially. Equally, the influence of content dissemination driven by algorithmic logic in the public opinion-forming space will require

careful observation of the effectiveness of the enforcement means presented in this report in the future and whether further adaptations might be unavoidable.

A publication
of the European Audiovisual Observatory