Visegrad Alliance
for Digital Rights
and Disinformation Defense

NATIONAL REPORT

HUNGARY

Legal framework as of November 30, 2025.

The project is co-financed by the governments of Czechia, Hungary, Poland, and Slovakia through Visegrad Grants from the International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

Visegrad Fund

ABOUT THE AUTHORS

Boldizsár Szentgáli-Tóth
Senior Research Fellow
Centre for Social Sciences

Boldizsár Szentgáli-Tóth is a distinguished constitutional law scholar specializing in comparative constitutional law and a senior research fellow at the Hungarian Academy of Sciences, specifically within the Centre for Social Sciences. His academic focus encompasses constitutional identity, artificial intelligence, the legal implications of crises such as the COVID-19 pandemic, and the relationship between constitutionalism and governance in the modern age. His expertise also extends to the analysis of qualified majority legislation and the protection of freedom of expression in the digital realm.

Rudolf Berkes
Project researcher
Centre for Social Sciences

Rudolf Berkes is a legal scholar and project researcher in constitutional and administrative law at the Centre for Social Sciences, Institute for Legal Studies. His research focuses on the constitutional and regulatory implications of artificial intelligence, with particular attention to algorithmic constitutionalism, parliamentary governance, and the interaction between emerging technologies and democratic institutions. His scholarly work also engages with issues of freedom of expression, automated decision-making, and the evolving role of legal scholarship in the context of EU-level digital regulation. Through his research and publications, he contributes to contemporary debates on how constitutional frameworks can adapt to technological transformation while safeguarding democratic values.

Orsolya Zita Ferencz
Research Assistant
Centre for Social Sciences

Orsolya Zita Ferencz is a Research Assistant at the Centre for Social Sciences. Her research focuses on constitutional review and intellectual property law.

1 LEGISLATION AND CASE-LAW CONCERNING DISINFORMATION AND HATE SPEECH

Attach the full range of public authority instruments, from criminal sanctions to administrative offences and other instruments, including noteworthy legislative proposals that did not pass.

1.1 Legal Framework and Definitions

Does your national legal framework define disinformation?

No general statutory definition of "disinformation" exists. The term appears in policy documents (e.g. government strategies on "fake news"), but Hungarian law does not provide a precise legal definition.

Does your national legal framework define hate speech?

Yes. While Act C of 2012 on the Criminal Code does not use the exact phrase "hate speech," it criminalises forms of expression that amount to hate speech: incitement against a community (Section 332), internet agression (Section 332/A) and use of symbols of totalitarian regimes (Section 335). Civil law also protects personal rights against hate speech.

Are there any specific distinctions made between online and offline disinformation or hate speech in your legislation?

No. The Criminal Code applies equally to online and offline expression. However, since January 1st 2025, Section 332/A of the Criminal Code explicitly extend criminal liability to online communications, strengthening the digital dimension.

1.2 Criminal Sanctions

Which criminal offences address disinformation in your jurisdiction (e.g., spreading false news, incitement, etc.)?

Section 337 of the Criminal Code addresses "Scaremongering" (*rémhírterjesztés*), which is the publishing or disseminating false facts capable of causing public panic. Section 337(2) aggravates penalties if the act occurs during a special legal order (e.g. state of emergency). This was notably used during the COVID-19 emergency against alleged fake news.

Which criminal offences address hate speech in your jurisdiction?

The following sections of the Criminal Code address hate speech in Hungarian jurisdiction:

- Section 332: Incitement against a community (stirring hatred against national, ethnic, racial, religious groups, or groups defined by disability, sexual orientation, gender identity).
- Section 332/A: Internet agression
- Section 335: Use of symbols of totalitarianism.

What are the typical penalties (fines, imprisonment, etc.) associated with these offences? (if available)

The penalties for these offences are the following:

- Scaremongering: up to 3 years' imprisonment, aggravated form up to 5 years.
- Incitement against a community: up to 3 years' imprisonment.
- Internet agression: up to 1 year imprisonment.
- Use of symbols totalitarianism: custodial arrest.

Are there any aggravating factors that increase penalties for disinformation or hate speech (e.g., content targeting vulnerable groups)?

For scaremongering, the penalties are higher during special legal orders (e.g. state of emergency, epidemic).

When sentencing, the court must take into account mitigating and aggravating circumstances according to Section 80 of the Criminal Code. In judicial practice, a racist, xenophobic, or discriminatory motive is regularly treated as an aggravating circumstance.

1.3 Administrative Offences and Civil Measures

Beyond criminal law, are there any administrative offences covering disinformation or hate speech?

Yes. The Act CIV of 2010 on the Freedom of the Press and Fundamental Rules of Media Content prohibits incitement to hatred and content that severely offends communities. The NMHH Media Council may impose administrative sanctions on

broadcasters, publishers, or online media for violations. In 2024, the Act LXXVIII of 2024 on the Suppression of Internet Aggression introduced new administrative measures for harmful online content.

What types of administrative penalties are imposed (e.g., fines, warning notices, temporary bans)?

Penalties include fines, suspension of programs or services, binding corrective measures, and in repeated or severe cases, revocation of licenses for media outlets. For online intermediaries under the Digital Services Act (DSA) framework, the NMHH (as Digital Services Coordinator) may issue orders, fines, and corrective obligations.

Are there civil law remedies (e.g., defamation suits, injunctions) available for victims or affected parties?

Yes. Under Act V of 2013 on the Civil Code, individuals may sue for violation of personality rights (including defamation, insult, or hate speech). Remedies include injunctions, publication of apologies, corrections, and monetary damages for pecuniary and non-pecuniary harm.

1.4 Scope of Instruments and Enforcement

Which public authorities or institutions are responsible for enforcing laws on disinformation and hate speech?

Criminal offences are investigated by the police and prosecuted by the Prosecutor General's Office and adjudicated by the courts.

Administrative offences are enforced mainly by the NMHH Media Council (broadcast/press/online media content) and now by NMHH as DSA coordinator.

Ordinary civil courts are responsible for civil law cases.

How do these authorities identify and investigate potential cases?

Criminal cases often start from police investigations triggered by reports or online monitoring.

NMHH acts on complaints, monitoring, or referrals (e.g., from trusted flaggers under the DSA).

Civil cases rely on private litigation initiated by victims.

Are there any specialized agencies or task forces focusing on online disinformation or hate speech?

No independent agency exists solely for disinformation. However, the NMHH has dedicated units monitoring online platforms, and during the COVID-19 pandemic, police set up special cyber units to track fake news. The 2024 Internet Aggression law suggests further institutional focus.

Could you provide any statistics or data on enforcement actions, prosecutions, or convictions?

Although the official statistics are sparse, during the COVID-19 emergency in 2020 and 2021, police reported over 100 investigations for scaremongering (rémhírterjesztés).

NMHH regularly reports dozens of administrative fines each year for media content violations, but specific numbers for hate-speech-related sanctions are not always disaggregated.

1.5 Case-Law and Judicial Interpretations

What are the most significant court decisions shaping the interpretation of disinformation or hate speech laws in your country?

- Hungarian Constitutional Court, Decision 96/2008 (VII.3.) AB: clarified that hate speech may justify restriction when it endangers human dignity and democratic order.
- Kúria (Supreme Court) cases on scaremongering confirmed that “false facts likely to cause public panic” must be narrowly construed.
- ECHR case – Magyar Tartalomszolgáltatók Egyesülete and Index.hu Zrt v. Hungary (2016): held Hungary liable for imposing liability on online news portals for third-party comments, shaping how intermediary liability applies.

Have any high-profile cases set important precedents regarding the enforcement of these laws?

Yes. COVID-era fake news prosecutions (2020) received international attention; though many cases were later dropped, they highlighted risks of overreach. The 2016 ECHR Index.hu case became a major precedent on liability for user comments.

How do courts balance the protection of society from disinformation or hate speech with the right to freedom of expression? Is the principle of proportionality the main instrument?

Yes. Both Hungarian ordinary courts and the Constitutional Court rely on the principle of proportionality: restrictions on expression must be necessary in a democratic society and proportionate to the harm. The ECHR's jurisprudence strongly influences this balancing, ensuring that only speech that genuinely endangers public order, dignity, or security can be sanctioned.

1.6 Legislative Proposals (Including Those Not Passed)

Have there been recent legislative proposals aimed at combating disinformation or hate speech? If so, what did they entail?

No targeted legislative proposals aimed to combat disinformation and hate speech. However indirectly, the government has started using the "influcencing of public discourse" as a pretext to implementing or proposing new legislation.

As part of the 'Authorisation Act' adopted on 30 March 2020, which introduced emergency rules in Hungary in response to the COVID-19 pandemic. Section 337 of the Criminal Code was permanently amended to extend the sentence for "fearmongering" to up to five years' imprisonment if it is "capable of obstructing the efficiency of protection efforts" during a "state of danger".

Recent legislation including the Sovereignty Protection Act (2023) empowers authorities to investigate "information manipulation and disinformation activities" affecting state decision-making. Following that, The most recent legislative proposal titled "On the Transparency of Public Life" (T/11923) targets media outlets and NGOs receiving foreign funding, including EU grants. The proposal would empower the Sovereignty Protection Office to blacklist organisations that try to "influence public discourse" via the help of foreign funding, without meaningful

judicial review. The bill is currently under consideration, after Fidesz parliamentary leader Máté Kocsis announced indefinite postponement "until autumn" following protests and resistance from professional organizations.

Were there any proposals that did not pass? If yes, what were the main reasons for their rejection or withdrawal?

The most recent legislative proposal titled “On the Transparency of Public Life” (T/11923) targets media outlets and NGOs receiving foreign funding, including EU grants. The proposal would empower the Sovereignty Protection Office to blacklist organisations that try to “influence public discourse” via the help of foreign funding, without meaningful judicial review. The bill is currently under consideration, after Fidesz parliamentary leader Máté Kocsis announced indefinite postponement "until autumn" following protests and resistance from professional organizations.

Did these proposals encounter notable opposition or controversy? If so, from which stakeholders?

Yes. The most recent legislative proposal titled “On the Transparency of Public Life” (T/11923) encountered heavy resistance from the society culminating in protests, from media and civil society organizations (Hungarian and international), from banking and other professional associations, and from the European Commission.

1.7 Role of Online Platforms and Intermediaries

Are there specific obligations (solely from state legislation, not enforced by EU law) placed on social media companies or digital platforms to monitor and remove disinformation or hate speech?

Hungarian domestic legislation places limited specific obligations on social media platforms, reflecting the government's stated preference for using EU law to regulation digital platforms.

What is the liability regime for internet service providers or online platforms in your jurisdiction?

Hungary's liability regime for internet service providers and online platforms is established through Act CVIII of 2001 on Electronic Commerce (E-Commerce Act), implementing the EU E-Commerce Directive.

Have any landmark cases or regulatory actions been taken against major tech platforms under these rules?

Hungarian authorities have pursued several landmark enforcement actions against major tech platforms, primarily through the Hungarian Competition Authority (GVH) using consumer protection and competition law.

The most significant case involved Facebook Ireland Limited, fined HUF 1.2 billion (€3.6 million) by the GVH in December 2019. The GVH found Facebook's "It's free and always will be" claims violated the Unfair Commercial Practices Directive, arguing users "paid" with their data rather than money. The authority established that Facebook's business model converted user data into advertising revenue, making "free" claims misleading. The case was ultimately unsuccessful: both the Metropolitan Court and Hungarian Supreme Court sided with Facebook, ruling the "free" claim was not misleading. The GVH even requested a preliminary ruling from the ECJ, which was rejected.

1.8 International and Regional Considerations

Has your country ratified or adopted any international conventions or regional directives relevant to disinformation or hate speech?

Hungary has ratified and implemented several key international conventions and regional directives addressing hate speech and disinformation.

Hungary ratified the International Convention on the Elimination of All Forms of Racial Discrimination (ICERD) in 1967, requiring criminalization of hate speech on racial grounds.

Hungary also ratified the International Covenant on Civil and Political Rights (ICCPR), binding the state to Article 20(2) obligations prohibiting incitement to hatred.

Hungary transposed Framework Decision 2008/913/JHA on combating racism and xenophobia through 2016 amendments to Criminal Code Section 332.

Hungary signed the Additional Protocol to the Cybercrime Convention concerning hate speech online.

How do these international obligations influence domestic legislation and case-law?

Hungary amended Criminal Code Section 332 in October 2016 specifically to comply with Framework Decision 2008/913/JHA and avoid EU infringement proceedings. The amendments added "incitement to violence" alongside hatred and extended protection to individual group members rather than groups only.

Are there any ongoing discussions about aligning national law with regional or global standards?

The Hungarian government is actively resisting any domestic or international discussion on aligning national law with regional or global standards on disinformation and hate speech. Hungarian authorities invoke "constitutional identity" and "national sovereignty" to resist EU compliance partially based on the Constitutional Court decision 22/2016 (XII. 5.) AB that established that Hungary can override EU law when it conflicts with constitutional identity, creating fundamental tensions with European integration.

1.9 Practical Challenges and Enforcement Gaps

Is there a notable gap between the laws on paper and the practical enforcement?

There is a substantial gap between Hungary's formal hate speech and disinformation laws and their practical enforcement. Hungarian criminal statistics reveal extremely low prosecution rates for hate crimes and incitement as a result of systematic investigative failures. Most criminal proceedings are terminated at the investigative phase, police apply very restrictive approaches to direct danger assessment, fail to question witnesses, collect CCTV evidence, or conduct proper background investigations, while prosecutors routinely refuse to press charges. This enforcement gap renders Hungary's hate speech framework largely symbolic rather than protective.

Are there examples of under-enforcement or over-enforcement in practice?

The deficiencies of the implementation is evidenced by the fact that the European Court of Human Rights (ECtHR) has already ruled in four hate crime cases represented by the Working Group Against Hate Crimes' members against

Hungary and in all cases established the violation of the European Convention of Human Rights.

Their report suggests that in all four cases the ECtHR found violations of the Roma applicants' fundamental rights in consequence of the omissions of law-enforcement authorities in proceedings related to bias motivated crimes. In the Balázs v. Hungary case (15529/12) the ECtHR found that the failure of the Hungarian authorities to investigate the hate motivation behind violence against a member of the Roma community which amounted to a violation of Article 14 in conjunction with Article 3 of the ECHR. In the case of R.B. v. Hungary (64602/12), the applicant claimed that the authorities failed to investigate her case and protect her from harassment motivated by racism, including verbal assaults and physical threats at an openly anti-Roma rally in her neighbourhood. The ECtHR found a violation of Article 8 of the ECHR concluding that the State failed to adequately protect her due to faulty implementation of the criminal law mechanisms. Similarly, in the Király and Dömötör v. Hungary case (10851/13) the ECtHR concluded that because of the numerous shortcomings in the implementation of the criminal law mechanisms, the applicants suffered an attack on their physical and psychological integrity, which constituted a violation of Article 8 of the ECHR. In the M.F. v. Hungary case (45855/12) the ECtHR found that the failure of the state authorities to examine the question of possible racial motives behind a violent crime committed by police officers in duty against a Hungarian national of Roma origin amounted to the violation of Article 14 in conjunction with Article 3 of the ECHR.

Hungarian authorities initiated 134 criminal investigations under COVID-19 scaremongering provisions, primarily targeting journalists questioning government preparedness.

2
ROLE OF AUTOMATIZATION AND AI IN CONTENT REGULATION

Have there been legal cases around deep fakes, synthesized speeches of politicians, etc.?

2.1 Legal Recognition and Definitions

Does your national legislation specifically define or recognize deep fakes or other AI-generated content (e.g., synthetic media)?

Hungarian national legislation does not specifically define or recognise deepfakes or other AI-generated content. The term "deepfake" does not appear explicitly in Hungarian regulatory frameworks. However, relevant provisions of Hungary's 2012 Criminal Code apply to crimes involving deepfakes, including harassment, defamation, and sexual blackmail.

Are there any legal provisions that explicitly address the creation, dissemination, or misuse of AI-generated content?

Hungarian legislation lacks explicit provisions addressing AI-generated content creation, dissemination, or misuse. However, existing Criminal Code provisions apply to deepfake-related crimes, including defamation (rágalmazás), harassment (zaklatás), sexual blackmail (szexuális kényszerítés), fraud (csalás), and identity misuse. The 2012 Criminal Code's general provisions cover situations where deepfakes cause harm to individuals' reputation or are used for criminal purposes.

2.2 Criminal and Civil Liability

Which criminal or civil offences (if any) apply to the production or distribution of deep fakes or similar synthetic media?

Hungarian legislation lacks explicit provisions addressing the production or distribution of deep fakes or similar synthetic media. Nevertheless several criminal and civil offences in Hungarian law apply to deepfake production and distribution. Criminal Code provisions include harassment (Article 222) when perpetrators send manipulated images to victims, defamation (Article 180) for reputation damage, personal data misuse (Article 219) when facial images are processed without

consent causing substantial damage, and sexual blackmail when deepfakes are used coercively. Civil remedies under Section 2:43 of the Civil Code protect personality rights including facial likeness violations, enabling claims for restitution without proving damage.

Have any cases been prosecuted under existing laws (e.g., defamation, identity theft, fraud) rather than new legislation targeting AI-generated content?

No recent Hungarian court decisions specifically address deepfakes or AI-generated content. However, Hungarian courts have decided analogous cases involving face-swapping technology that could provide precedential guidance. Notable related decisions include the Supreme Court's Pfv.21.267/2018/17 judgment, which examined whether a plaintiff's image rights were violated when their face was digitally montaged onto sexually explicit content without consent. Similarly, the Metropolitan Court of Appeal ruled in Pf.21.277/2008/3 on comparable image manipulation issues.

2.3 Preventive Measures and Oversight

Are there requirements for AI developers or platform operators to label or disclose AI-generated content?

Hungarian law requires AI developers and platform operators to label AI-generated content under EU AI Act Article 50, implemented domestically since February 2025. Specifically, providers of AI systems generating synthetic audio, image, video, or text content must ensure outputs are marked in machine-readable and detectable formats. The labeling must be "clear and unambiguous" and provided "at the latest at the time of the first interaction". The Hungarian government established an implementation framework through Government Decision 1301/2024, creating a new Hungarian Artificial Intelligence Office to enforce these obligations.

Have any policy initiatives or industry self-regulation measures been introduced to mitigate harms associated with deep fakes?

Hungary has introduced several notable policy initiatives and industry self-regulation measures to address AI-generated content and deepfake harms. Government policy initiatives include Hungary's updated AI Strategy 2025-2030,

released in September 2025, which establishes a comprehensive framework for responsible AI development and includes annual review mechanisms to address technological developments. The government established the Hungarian Artificial Intelligence Office through Decision 1301/2024 to oversee implementation of EU AI Act requirements. The Hungarian Competition Authority (GVH) conducted market analysis recommending targeted interventions to support SME adoption of AI technologies whilst protecting consumers.

Hungarian media and marketing communication organisations published the first comprehensive AI handbook in April 2025, developed by the Association of Hungarian Communication Agencies (MAKSZ), Hungarian Newspaper Publishers Association (MLE), and Hungarian Marketing Association (MMSZ). This 107-page handbook addresses ethical, legal, and regulatory frameworks for AI use, including content labelling, copyright issues, and data security protocols.

Are there any mandatory or voluntary codes of practice for social media platforms regarding AI-generated content?

Hungarian law establishes both mandatory and voluntary frameworks for social media platforms regarding AI-generated content. Mandatory obligations derive primarily from EU Digital Services Act (DSA) implementation, with the National Media and Infocommunications Authority (NMHH) serving as Hungary's designated Digital Services Coordinator since January 2023. The EU AI Act's General-Purpose AI Code of Practice provides additional voluntary compliance mechanisms, offering reduced regulatory scrutiny for signatory platforms.

2.4 Impact on Political Processes and Elections

Have there been instances where deep fakes or AI-generated speeches impacted election campaigns, political debates, or voter perceptions?

Hungary has experienced multiple instances of deepfakes and AI-generated content impacting political campaigns, particularly involving Fidesz (the ruling party) and targeting opposition politicians. The most documented cases occurred during the 2024 European Parliament election campaign, where Fidesz extensively deployed AI-generated propaganda against opposition leader Péter Magyar. Proxy organizations of Fidesz are currently scaling up the use of AI-generated videos ahead of the upcoming 2026 general elections. These became a primary political communication tool in the online space. Opposition parties used AI-generated

images sparingly during the last 18 months. Exact impact on voter perception is difficult to determine, given the already existing high political polarization in the country.

How do electoral regulations or campaign laws address the use of AI-generated media (e.g., transparency rules, disclaimers)?

Hungarian electoral regulations contain no specific provisions addressing AI-generated media transparency or disclosure requirements. Act XXXVI of 2013 on Election Procedure lacks explicit AI content labeling obligations, whilst Section 149's general consent requirements for voter contact do not encompass synthetic media.

2.5 Future Outlook and Emerging Trends

Are there legislative proposals pending or under discussion that aim to address deep fakes or AI-generated disinformation more explicitly?

As of September 2025, no specific legislative proposals targeting deepfakes or AI-generated disinformation are pending in the Hungarian National Assembly. Current regulatory approach relies on EU AI Act implementation through Government Decision 1301/2024, establishing the Hungarian Artificial Intelligence Office with general oversight responsibilities.

3
THE PROHIBITION OF CENSORSHIP AND ITS IMPACT ON REGULATING INTERNET CONTENT AND DISINFORMATION

3.1 Constitutional and Legislative Framework

Does your country's constitution or primary legislation explicitly prohibit censorship? Are there exceptions or limitations to the prohibition on censorship (e.g., national security, public order)?

Hungary's constitution does not explicitly prohibit censorship but provides qualified protection for freedom of expression under Article IX of the Fundamental Law. Article IX(1) guarantees "everyone shall have the right to freedom of expression," whilst paragraph (2) recognizes press freedom and information diversity. However, these rights contain inherent limitations. Article IX(4) restricts freedom of expression, stating it "cannot be aimed at violating other persons' human dignity". The Fourth Amendment (2013) further limits expression that violates "the dignity of the Hungarian nation or of any national, ethnic, racial or religious community". Special legal order provisions (Articles 52-54) permit substantial restrictions during emergencies. Article 52(2) allows suspension or restriction of fundamental rights beyond normal constitutional limits, excluding only human dignity, right to life, and specific procedural rights.

As part of the 'Authorisation Act' adopted on 30 March 2020, which introduced emergency rules in Hungary in response to the COVID-19 pandemic, Section 337 of the Criminal Code was permanently amended to extend the sentence for "fearmongering" to up to five years' imprisonment if it is "capable of obstructing the efficiency of protection efforts" during a "state of danger". Recent legislation including the Sovereignty Protection Act (2023) empowers authorities to investigate "information manipulation and disinformation activities" affecting state decision-making.

3.2 Judicial Interpretations and Key Cases

What major court decisions have clarified the boundaries of censorship, particularly in relation to online speech?

The Hungarian Constitutional Court's Decision 19/2014 addressed intermediary liability for user-generated content, ruling that online platforms could be held liable for offensive comments even without editorial knowledge of publication. The majority decision emphasised that Article IX of the Fundamental Law requires balancing freedom of expression against human dignity protection. However, Judge István Stumpf's dissenting opinion advocated for a more proportionate "notice and takedown" system, arguing that strict liability created unacceptable chilling effects on online discourse.

The MTE v. Hungary judgment (2016) marked a pivotal correction to Hungarian practice. The ECtHR ruled that Hungarian courts violated Article 10 by imposing objective liability on Magyar Tartalomszolgáltatók Egyesülete and Index.hu for user comments. The Court emphasised that liability assessments must involve proper balancing between competing rights, distinguishing "clearly unlawful speech" from merely offensive content.

Subsequently, Magyar Jeti Zrt v. Hungary (2018) addressed hyperlink liability, with the ECtHR condemning Hungarian courts' imposition of strict liability for links directing users to defamatory YouTube content. The Court established that hyperlinking constitutes directing rather than providing content, making absolute liability disproportionate under Article 10.

Have any pivotal judgments addressed the tension between prohibiting censorship and controlling disinformation?

As part of the ‘Authorisation Act’ adopted on 30 March 2020, which introduced emergency rules in Hungary in response to the COVID-19 pandemic, Section 337 of the Criminal Code was permanently amended to extend the sentence for “fearmongering” to up to five years’ imprisonment if it is “capable of obstructing the efficiency of protection efforts” during a “state of danger”. The Constitutional Court, in Decision No. 15/2020. (VII. 8.) AB found that the provisions met constitutional requirements.

The ATV Zrt v. Hungary case before the European Court of Human Rights illustrated domestic courts' approach to balancing media bias concerns against expression rights. Hungarian authorities fined ATV television for labelling a political party "far-right" without providing balanced coverage, arguing this violated unbiased reporting requirements under the Media Act. Considering the lack of clarity in the legislation and the divergent approaches by domestic courts, the ECtHR found the interference disproportionate and not necessary in a democratic society. Therefore, it concluded that ATV's right to FoE under Article 10 ECHR was violated.

3.3 Scope and Enforcement

Which authorities or regulatory bodies are responsible for enforcing the prohibition on censorship?

The Hungarian Constitutional Court serves as the primary guardian of constitutional rights, including Article IX freedom of expression protections. The Court reviews legislation for constitutional compliance and has issued pivotal decisions on media regulation, including Decision 19/2014 on internet liability and rulings striking down parts of the 2010 Media Act. Hungarian courts adjudicate censorship cases through both constitutional review and ordinary litigation. The European Court of Human Rights provides external oversight, as demonstrated in MTE v. Hungary and Magyar Jeti cases establishing boundaries for intermediary liability.

National Media and Infocommunications Authority (NMHH) functions as Hungary's media regulator and Digital Services Coordinator since January 2023. The Authority enforces DSA content moderation requirements and investigates platform compliance with transparency obligations.

Hungary's Parliamentary Commissioner for Fundamental Rights (ombudsman) monitors fundamental rights violations and investigates public administration complaints. The Commissioner surveys freedom of expression infringements and submits annual reports to Parliament.

How do these bodies reconcile the prohibition with the need to remove unlawful or harmful content (e.g., hate speech, false information)?

The Hungarian Constitutional Court applies proportionality tests derived from European Court of Human Rights jurisprudence, requiring restrictions to be "necessary and proportionate to the aim pursued". Following the Fourth Amendment (2013), Article IX(5) of the Fundamental Law explicitly permits restrictions where expression "violates the dignity of the Hungarian nation or any national, ethnic or religious community". The Court balances competing rights through case-by-case assessment, examining whether restrictions serve legitimate aims and employ least restrictive means.

Hungary's E-Commerce Act provides detailed notice-and-takedown procedures for copyright infringement and personality rights violations, offering alternatives to lengthy court proceedings. The Act requires intermediaries to act expeditiously upon notification whilst maintaining limited liability protections for passive transmission. The NMHH, serving as Digital Services Coordinator, implements DSA transparency requirements mandating platforms provide clear "statements of reasons" for content restrictions, disclosure of automated decision-making, and appeals mechanisms. Authorities distinguish between "illegal" and "harmful" content, with different procedural requirements. Illegal content (hate speech, incitement) requires immediate removal following court orders or independent adjudication, whilst harmful content involves discretionary platform policies subject to transparency obligations.

What measures ensure that internet regulations do not amount to de facto censorship?

Users possess three-tiered appeal rights: platform internal review, national regulatory oversight through the NMHH, and Appeals Centre Europe (ACE) providing independent supranational review.

The Digital Services Act implementation mandates detailed transparency obligations for content moderation. Platforms must provide "statements of reasons" for content restrictions, disclose automated decision-making processes, and maintain public databases of moderation actions. The NMHH publishes annual reports documenting platform compliance and content removal statistics.

Hungarian law requires notice-and-takedown procedures with clear timelines and justification requirements.

Hungarian courts apply proportionality testing derived from European Court of Human Rights jurisprudence, examining whether restrictions are "necessary and proportionate to the aim pursued". The Hungarian Constitutional Court conducts comprehensive reviews of content regulation measures, as demonstrated in Decision 19/2014 on intermediary liability. Courts must demonstrate that less restrictive alternatives were considered and that measures serve legitimate aims. European Court of Human Rights supervision provides ultimate safeguards, as shown in MTE v. Hungary and Magyar Jeti cases establishing strict liability limits. European Commission infringement proceedings constrain excessive national restrictions, particularly regarding proportionality violations.

3.4 Practical Outcomes and Challenges

Are there instances where the prohibition of censorship resulted in the inability to remove content widely considered harmful or misleading?

The most documented phenomenon involves systematic under-enforcement of existing hate speech laws by Hungarian law enforcement. The European Commission against Racism and Intolerance (ECRI) reports that "strict judicial interpretation of legal requirements" severely limits the effectiveness of hate speech frameworks. Hungarian courts apply restrictive standards that effectively prevent content removal even where legislation theoretically permits intervention. The Constitutional Court's approach to incitement requires demonstrating "manifest and imminent danger," creating high thresholds rarely met in practice.

As part of the ‘Authorisation Act’ adopted on 30 March 2020, which introduced emergency rules in Hungary in response to the COVID-19 pandemic, Section 337 of the Criminal Code was permanently amended to extend the sentence for “fearmongering” to up to five years’ imprisonment if it is “capable of obstructing the efficiency of protection efforts” during a “state of danger”. The Constitutional Court, in Decision No. 15/2020. (VII. 8.) AB found that the provisions met constitutional requirements. Despite these changes, misleading health information continued to circulate essentially unchecked.

Conversely, are there examples of state overreach where content was restricted under the guise of public interest, raising censorship concerns?

As part of the 'Authorisation Act' adopted on 30 March 2020, which introduced emergency rules in Hungary in response to the COVID-19 pandemic, Section 337 of the Criminal Code was permanently amended to extend the sentence for "fearmongering" to up to five years' imprisonment if it is "capable of obstructing the efficiency of protection efforts" during a "state of danger". The Constitutional Court, in Decision No. 15/2020. (VII. 8.) AB found that the provisions met constitutional requirements. In general however, the Hungarian government used mainly indirect approaches to silence criticism and journalism, instead relying on direct censorship. These approaches include media regulation, media capture, and targeted surveillance of investigative journalists.

3.5 Future Outlook

Are there ongoing discussions about refining or reinterpreting the prohibition on censorship to account for evolving digital challenges?

Hungarian legal scholars are actively examining digital constitutionalism and platform regulation challenges. Legal experts are debating whether traditional constitutional frameworks adequately address emerging digital challenges, particularly regarding platform content moderation and state sovereignty claims.

Substantive public discussion is limited, as most media coverage had been focused on the proposed, then sidelined, legislation on the "transparency of public life". The bill would have empowered the Sovereignty Protection Office to blacklist organisations receiving foreign funding without meaningful judicial review. After public outrage, the governing party postponed parliamentary debates on the proposal.

What emerging technologies (e.g., AI-driven content moderation) might influence future debates on censorship and disinformation regulation?

The spread of AI-generated political content during the current electoral campaign ahead of the 2026 parliamentary elections could prompt discussions on regulation. In addition the widespread use of disinformation by political actors in the last decade could also inspire such debates and regulation.

4
NATIONAL REGULATION OF INTERNET CONTENT

Especially website blocking, social media/platforms regulation, not limited solely to EU-based regulation; legislation, case law and effectivity analysis.

4.1 Legislative Framework

What laws or regulations govern the blocking of websites and the regulation of social media/platforms in your country?

The primary laws and regulations governing the blocking of websites and the regulation of platforms in Hungary are the following:

- Act CVIII of 2001 on Electronic Commerce;
- Hungary's national implementing act for the EU Digital Services Act ("DSA") (Act CIV of 2023 and related NMHH enforcement decrees);
- provisions in the Criminal Code and sectoral laws that enable removal/blocking of unlawful content;
- NMHH (the National Media and Infocommunications Authority) rules and decisions.

4.2 Scope of Website Blocking

Under what circumstances can websites be blocked (e.g., illegal content, piracy, national security concerns)?

Typical grounds include hosting illegal content (child sexual abuse material, certain hate/ Holocaust-denial offences, criminal content, piracy/ copyright infringements where judicial orders apply), court-ordered removals, and actions taken under national public-interest or criminal procedures. At platform level, the DSA creates removal duties for illegal content and procedures for public authorities and trusted flaggers. Practical blocking in Hungary has been used where content is found unlawful by courts or under criminal procedures.

Could it be said that the legislation on website blocking leaves a lot of discretion to the blocking authority, and so the provision of the law is very broad?

While the DSA introduces detailed obligations for platforms, Hungary's domestic framework still leaves considerable discretionary space: courts, prosecutors, and administrative bodies (and under the DSA the NMHH) have broad levers to require removal or to seek ISP blocking, and watchdogs have flagged that some enforcement powers and appointment of the NMHH raise concerns about wide administrative discretion.

Is it conceivable that a court or administrative body would block a website on an ad hoc basis, on the basis of a very general mandate? E.g. interim measures in litigation.

Yes. Hungarian courts historically can order content to be made inaccessible and may issue interim measures in litigation. Under the DSA, NMHH also has administrative enforcement tools and can issue orders to intermediaries in specific cases. So ad-hoc/interim blocking by courts or administrative bodies is legally conceivable and has precedents in practice.

Who has the authority to order or implement website blocking (e.g., courts, government agencies, telecom regulators)?

Courts (civil/criminal injunctions and interim orders), prosecutors in criminal procedures, the ministerial/administrative channels used for cross-border cases, and now NMHH as the national Digital Service Coordinator for DSA enforcement. ISPs and/or hosting providers implement technical blocking when ordered.

Could it be said that the website blocking bodies are well staffed for this agenda?

No, staffing and enforcement capacity appear limited. The NMHH (now Hungary's DSA Digital Service Coordinator) publishes small complaint volumes and activity reports. Watchdogs repeatedly note that NMHH and other bodies operate with constrained resources and that enforcement is selective.

Is there a transparent process or published criteria for determining which sites get blocked?

Partially. Hungary maintains a central database of court-ordered inaccessibility decisions (Központi elektronikus hozzáférhetetlenné tételi határozatok adatbázisa, KEHTA) and the Electronic Commerce Act sets notice-and-action rules, but public criteria are limited and civil society has criticised transparency and scope of administrative discretion.

4.3 Implementation and Enforcement

How is website blocking technically enforced (e.g., DNS blocking, IP blocking, URL filtering)?

All common methods are used in practice in Hungary: DNS tampering/response blocking, IP-level blocking, and (where available) URL/path filtering or proxy blocking, with collateral blocking risks (domain-level blocks affecting many subpages).

Are there procedural safeguards (e.g., judicial warrants, due process) before blocking is executed?

Yes, where blocking follows court orders there are judicial procedures and the Electronic Commerce Act's notice/removal procedures offer administrative remedies. However, interim measures and administrative orders can create rapid takedowns/blocking.

Do the owners or operators always have the possibility to prevent the blocking of websites, e.g. are they given a period of time to correct illegal content?

Not always, but in most non-emergency cases yes. The Electronic Commerce Act sets notice-and-action procedures, and the DSA introduces complaint/counter-notice routes and redress. This gives platforms/hosts time and procedural steps to act. Emergency or criminal procedures and interim injunctions can lead to faster blocking where corrective windows may be short or absent.

Do the blocking authorities differentiate between blocking an entire website and blocking only part of a website?

Legally, targeted measures are preferable and the law contemplates targeted removal. However, in practice courts sometimes implement domain-level blocking, especially where targeted measures are technically difficult. It must also be highlighted, that EU case law stresses proportionality and prefers narrow measures when feasible.

How is the delivery of these warrants to other countries ensured?

Cross-border enforcement relies on EU cooperation mechanisms, namely DSA cooperation between national DSCs and the European Board. In criminal cases, traditional mutual-legal-assistance or judicial-cooperation channels are used. For platform content where the provider is established in another Member State, NMHH typically forwards complaints to the provider's DSC (per DSA rules) rather than issuing direct cross-border takedown warrants.

4.4 Transparency and Accountability

Are authorities required to publish lists of blocked websites and provide justifications for blocking decisions?

Court-ordered blocking decisions are entered into the Central Electronic Register of Blocking Orders (KEHTA), which is publicly accessible. The register records the decision and the legal ground, but justifications are generally brief. Administrative transparency is limited, and NGOs have flagged that explanatory detail is often lacking.

Do affected website owners, users, NGOs or public have avenues to challenge blocks or content removals before courts?

Yes. Website owners and affected parties can challenge blocking orders in Hungarian courts through appeal mechanisms or constitutional complaint. Under the DSA, users also have redress options in court if content or accounts are removed without lawful basis.

Do affected website owners, users, NGOs or public have avenues to challenge blocks or content removals before (administrative) bodies?

Yes, to some extent. The NMHH, as DSC, must provide procedures for complaints, out-of-court dispute resolution, and DSA-based administrative review. NGOs or individuals can submit complaints to NMHH if they consider a platform's moderation decision or a blocking action unlawful. Effectiveness, however, has been questioned by civil society.

Does the website blocking mechanism ensure that the blocking is always temporary?

Blocking ordered by courts or prosecutors remains in force until lifted or the underlying illegality ceases. Some blocks are time-limited (e.g., interim injunctions), but others can be effectively permanent if no appeal succeeds. There is no general rule that all blocks must expire automatically.

What mechanisms exist for independent review or oversight of blocking actions and platform moderation practices?

In this regard, the following must be mentioned:

- Courts (appeals, judicial review);
- Constitutional Court (constitutional complaints);
- NMHH supervision under the DSA (including annual reporting and EU-level Board cooperation);
- Ombudsman, who can investigate human-rights implications.

4.5 Impact and Effectiveness

Have any studies or official reports evaluated the effectiveness of website blocking or social media regulations in reducing unlawful or harmful content?

Yes. Academic and policy studies show mixed results: targeted blocking can reduce traffic to illegal/piracy sites but is often only *partly* effective and depends on dynamic injunctions, technical method and co-operation with intermediaries. Hungary's NMHH publishes hotline/enforcement reports, and broader EU/WIPO and academic evaluations (e.g., Carnegie Mellon, WIPO) have examined

effectiveness and stressed the need for adaptable, fast procedures to maintain impact.

How do blocked entities or individuals typically respond (e.g., mirror sites, VPN usage), and does this undermine the intended impact?

Common responses include deploying mirror sites, using proxies or VPNs, switching domains, or moving to alternative platforms. These behaviours reduce the impact of blocking and mean injunctions must be adaptive and coordinated with search engines, CDNs and platforms to remain effective. Empirical and technical studies show circumvention reliably undermines absolute effectiveness.

How do ISPs, platform operators, or tech companies influence the shaping of internet regulation?

They influence it by lobbying, participating in regulatory consultations, joining industry coalitions, and providing technical input on feasibility and costs. The NMHH's stated strategy shows formal structures or intent for stakeholder engagement (platforms, providers). The studies commissioned by NMHH show that the authority is gathering data on how platforms moderate content, which is a kind of consultation/oversight of platform practices. However, there is contest over how independent or how much influence industry has vs. political oversight (criticism that NMHH is too close to government). So the influence is there, but not necessarily with strong checks or balance.

4.6 Emerging Trends and Future Outlook

Are there any recent or upcoming legislative proposals that aim to broaden or narrow website blocking or social media regulation?

Yes, several recent Hungarian laws and proposals have changed online-content regulation in 2024 and 2025. Act LXXVIII of 2024 on Suppression of Internet Aggression (entered into force on 1 Jan 2025) and other 2024 measures (e.g., child-protection/porn restrictions, Act XLIX of 2024) that expand criminal or administrative tools against online content. Additional draft bills (e.g., proposals targeting foreign-funded NGOs/expanded supervisory powers) have been reported in 2024 and 2025 and could further broaden administrative reach.

4.7 Practical and Ethical Considerations

Have concerns been raised about over-blocking (collateral censorship) or chilling effects on legitimate speech?

Multiple watchdogs, NGOs and research studies warn that broad or imprecise blocking causes collateral damage, chilling and self-censorship. These concerns have been raised repeatedly in Hungary by Amnesty, Freedom House and academic commentators. Technical studies also stress collateral risk and recommend proportional, narrowly-targeted measures plus judicial oversight.

5
NATIONAL IMPLEMENTATION OF RELEVANT EU REGULATIONS CONCERNING INTERNET CONTENT

Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online

Regulation (EU) 2022/2065 (DSA)

(It is also possible to refer to other relevant European legislation.)

5.1 Transposition and Legislative Adaptation

Has your country adopted or adapted any national legislation to comply with Regulation (EU) 2021/784 on terrorist content online?

Act CXLII. of 2021. amending certain laws for the purpose of legal harmonisation in order to establish the interoperability of EU information systems in the fields of borders, visas, police and judicial cooperation, asylum and migration (https://njt.hu/jogszabaly/2021-142-00-00) added a new § 12/B. to act CVIII. of 2001. on certain issues of electronic commerce services and information society services (https://net.jogtar.hu/jogszabaly?docid=a0100108.tv). This new § 12/B. nominated the National Media and Infocommunications Authority as the Hungarian national authority responsible for the new tasks established by EU Regulation 2021/784.

Based on this statutory authorization, the president of the National Media and Communications Authority issued the new organizational and Operational Regulations of the Authority, which stipulates in its section 16.2. point f), that the communications defense department of the Authority shall perform all tasks imposed upon the Authority as the national contact point under EU Regulation 2021/784. Moreover, the same department shall manage all relevant procedures prescribed by EU Regulation 2021/784.

Apart from this, Annex. 3. of the Organizational and Operational Regulation renders the rules applicable in the operation of Internet Hotline, a legal service run by the Authority. Point 12. of Annex 3. provides that if any communication is suspected to be classified as terrorist content under EU2021/784, the Internet Hotline shall forward the case to the competent authority for further investigation.

What specific laws or regulations have been enacted or amended to align with the DSA (Regulation (EU) 2022/2065)?

The Hungarian Parliament has enacted Act CIV/2023. on on certain rules of internet mediation services, which contains the detailed rules of implementing EU Regulation 2022/265. (DSA): https://njt.hu/jogszabaly/2023-104-00-00

The National Media and Infocommunications Authority shall perform the tasks imposed by EU Regulation 2022/265 on national authorities in close collaboration with the National Data Protection Authority and the National Competition Authority.

5.2 Institutional Responsibilities

Which national authority or authorities are responsible for overseeing and enforcing compliance with the terrorist content regulation?

The amended text of § 12/B. (1) of act CVIII. of 2021. provides that the Hungarian National Media and Infocommunications Authority shall perform the new tasks established by EU Regulation 2021/784.

Similarly, which body (or bodies) monitors and enforces the Digital Services Act in your jurisdiction?

According to act CIV. of 2023. The National Media and Infocommunications Authority monitors and enforces EU Regulation 2022/265 in close collaboration with the National Data Protection Authority and the National Competition Authority.

Have any new regulatory agencies or units been created to handle these mandates?

No, new tasks have been allocated to an already existing authority.

5.3 Obligations for Hosting Service Providers

Under Regulation (EU) 2021/784, how are hosting service providers required to remove or disable terrorist content?

No specific rules have been established in Hungary. Act CVIII. of 2001. § 12/B. (2) provides, that The procedure referred to in Articles 3 to 5 of Regulation (EU) 2021/784 of the European Parliament and of the Council shall be conducted by the National Media and Infocommunications Authority, unless otherwise provided for in this Act, on the basis of the Act on General Administrative Procedure, in accordance with the rules of ex-office procedures. (3) adds that the decision of the Office taken in the procedure referred to in paragraph (2) may be challenged by administrative lawsuits before a court by a hosting service provider referred to in Article 2(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council, or by a content service provider referred to in Article 2(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council,

within three days of becoming aware of the decision. There is no immediate legal protection in the proceedings. The Office shall forward the statement of claim to the court within three days of its submission. The court shall adjudicate the application for legal remedy in a simplified trial within eight days of the receipt of the statement of claim by the court. There shall be no right to retrial against the court's judgment.

According to § 12/B. (5) in the event of a hosting service provider committing an infringement as defined in Article 18(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council, the Authority shall, with the exception specified in paragraph (6), act in accordance with the rules of the general regulatory supervision procedure and shall be entitled to apply the following legal consequences:

a) prohibit the infringement and impose an obligation in order to enforce the requirements of Regulation (EU) 2021/784 of the European Parliament and of the Council, and

b) impose a fine, as defined in Article 18(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council, of up to 4% of the total worldwide turnover of the preceding financial year, or

bb) – if the application of subparagraph ba) is not possible due to the lack of the necessary data – of up to one hundred million forints.

(6) stipulates that a warning shall not be issued for infringements as defined in Article 18(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council.

Are there specific timeframes for removal (e.g., the one-hour rule) and how are these enforced in practice?

The Hungarian legislation does not determine a specific deadline. Online service providers shall remove illegal content without delay, if the illegal content was reported for the service provider or any competent authority declares the content as illegal.

Regarding the DSA, what additional obligations (e.g., risk assessments, transparency reports) must online platforms fulfill in your country?

The National Media and Infocommunications Authority may order the release of certain data kept by the service providers. Besides this, the Authority may request from service providers to submit action plans or reports. The service providers may initiate administrative lawsuit against the imposition of these duties within 15 days. Hungarian online platform providers shall also pay a supervision fee for the authority which amounts to 0,25% of the last annual income of the service provider.

5.4 Notification and Removal Procedures

What procedures or protocols must authorities follow when issuing removal orders for terrorist content?

The relevant Hungarian rules are stipulated by §12/B. of Act CVIII. of 2023 as already outlined.

How do national courts or administrative bodies review such orders to ensure they are lawful and proportionate?

No specific rules have been established in Hungary. Act CVIII. of 2001. § 12/B. (2) provides, that The procedure referred to in Articles 3 to 5 of Regulation (EU) 2021/784 of the European Parliament and of the Council shall be conducted by the National Media and Infocommunications Authority, unless otherwise provided for in this Act, on the basis of the Act on General Administrative Procedure, in accordance with the rules of ex-office procedures. (3) adds that the decision of the Office taken in the procedure referred to in paragraph (2) may be challenged by administrative lawsuits before a court by a hosting service provider referred to in Article 2(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council, or by a content service provider referred to in Article 2(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council, within three days of becoming aware of the decision. There is no immediate legal protection in the proceedings. The Office shall forward the statement of claim to the court within three days of its submission. The court shall adjudicate the application for legal remedy in a simplified trial within eight days of the receipt of the statement of claim by the court. There shall be no right to retrial against the court's judgment.

According to § 12/B. (5) in the event of a hosting service provider committing an infringement as defined in Article 18(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council, the Authority shall, with the exception specified in paragraph (6), act in accordance with the rules of the general regulatory supervision procedure and shall be entitled to apply the following legal consequences:

a) prohibit the infringement and impose an obligation in order to enforce the requirements of Regulation (EU) 2021/784 of the European Parliament and of the Council, and

b) impose a fine, as defined in Article 18(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council, of up to 4% of the total worldwide turnover of the preceding financial year, or

bb) – if the application of subparagraph ba) is not possible due to the lack of the necessary data – of up to one hundred million forints.

(6) stipulates that a warning shall not be issued for infringements as defined in Article 18(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council.

Under the DSA, how are notice-and-action mechanisms implemented, and are there clear guidelines for both users and platforms?

The Authority will maintain a public register of relevant dispute resolution bodies, and trusted whistleblowers under the DSA Regulation.

In the event of a breach of the service provider's own terms and conditions or against the service provider's decision or action, the service user may initiate civil proceedings in accordance with the above Hungarian law, before the court of his/her place of residence (including foreign consumers). It is also possible to initiate an official supervisory procedure against a Hungarian service provider. Service providers are liable to users in accordance with the rules for damages caused by breach of contract.

The National Media and Infocommunications Authority created Internet Hotline: https://nmhh.hu/internethotline/dsa

This is a special legal service available for everyone through which potential notices could be easily communicated towards the Authority. Internet Hotline has been already registered as a trusted European whistleblower.

Act CVIII of 2023 also establishes an online dispute resolution platform, the decisions of which will be binding on the service provider if it has recognized it as binding on it (similar to the consumer online dispute resolution platform). Otherwise, the board will make a recommendation, the implementation of which must be proven. If the service provider does not implement the recommendations, the board will make this public.

5.5 Sanctions and Penalties

What sanctions or penalties can be imposed on service providers for non-compliance with Regulation (EU) 2021/784?

According to Act CVIII. of 2001. § 12/B. (5) in the event of a hosting service provider committing an infringement as defined in Article 18(1) of Regulation (EU) 2021/784 of the European Parliament and of the Council, the Authority shall, with the exception specified in paragraph (6), act in accordance with the rules of the general regulatory supervision procedure and shall be entitled to apply the following legal consequences:

a) prohibit the infringement and impose an obligation in order to enforce the requirements of Regulation (EU) 2021/784 of the European Parliament and of the Council, and

b) impose a fine, as defined in Article 18(2) of Regulation (EU) 2021/784 of the European Parliament and of the Council, of up to 4% of the total worldwide turnover of the preceding financial year, or

bb) – if the application of subparagraph ba) is not possible due to the lack of the necessary data – of up to one hundred million forints.

Under the DSA, are there specific ranges of fines or penalties that apply to infringements in your country?

In the event of a service provider's violation, the authority may apply the legal consequences specified in the law, taking into account gradualness and proportionality. Thus, in mild cases, it may establish the violation, order the cessation of conduct or even certification. It is important that mild legal consequences cannot be applied in the event of a repeated violation. In addition, the authority may prohibit the violating conduct, impose a fine, or even order the publication of a notice.

In terms of fines, the law has set a maximum fine, which is 1% for procedural fines (e.g. providing false data, withholding information), 6% in other cases or 5% for daily fines, and the fine is based on the service provider's global financial turnover in the previous year. If there is no data for the latter, or – in some cases – if the offender is a natural person, then itemized amounts according to the law are taken into account, which can be up to 100 million forints. In some cases, senior officials can also be fined (generally with fines ranging from 50 thousand forints to 3 million forints), or the authority can apply sanctions together.

Have there been any notable enforcement actions or penalties imposed so far?

No major enforcement actions have been registered so far. According to the Hungarian Digital Services Coordinator's 2024 annual activity report, the Hungarian National and Infocommunications Authority received 12 complaints until the end of 2024, all related to very large online platforms (VLOPs) established outside Hungary, and these complaints were forwarded to the Digital Services Coordinators of establishment, primarily to the Irish DSC.

5.6 Scope and Application

Are all online platforms equally subject to these regulations, or do smaller platforms and start-ups have different obligations?

According to act CIV. of 2023, smaller platforms and start-ups are exempted from the payment of the aforementioned supervision fee.

Does your country apply any specific exemptions or streamlined procedures for non-profit platforms, academic repositories, or other niche services?
No such exemptions have been established.

5.7 Judicial Review and Legal Challenges

Have there been any court cases challenging the implementation or scope of Regulation (EU) 2021/784 in your jurisdiction?
No such cases have been initiated so far.

Regarding the DSA implementation, some members of the European Parliament addressed a letter to the European Commission expressing concernes related to the independence of the appointed Hungarian implementing authority: https://dig.watch/updates/hungarys-appointed-dsa-authority-raises-concerns-in-brussels

Besides this, the European Court of Justice ruled on the Case C-46/23 Újpesti Polgármesteri Hivatal on March 14, 2024, which involved a data protection challenge against a Hungarian municipality (Újpest), confirming the Hungarian Data Protection authority's right to order data erasure even without a prior request from the data subject. This case, while not related to the Digital Services Act (DSA), highlights legal activity in Hungary concerning digital regulation and data protection, specifically under the GDPR.

What arguments—constitutional, procedural, or otherwise—have been raised in these challenges?
No information stands at our disposal.

5.8 Transparency and Reporting

Do authorities or platforms publish reports on the volume of terrorist content removed under Regulation (EU) 2021/784?
The Hungarian Media and Infocommunications Authority publishes an annual activity report, however, this contains only more general information on digital service moderation rather than specific data from the removed terrorist content under EU Regulation 2021/784.

Under the DSA, what transparency requirements exist for service providers (e.g., content moderation reports)?
By general terms, online service providers shall not submit reports from content moderation to the National Media and Infocommunications Authority, however, the Authority may order such reporting for certain service providers if systemic non-

compliance with requirements set by the DSA is suspected. Apart from this, upon call of the Authority, online service providers shall provide the required data to the Authority. Online service providers may submit administrative lawsuit to the judiciary within 15 days of receipt the order.

How accessible is this information to the public or civil society watchdogs?

The reports from online service providers submitted to the Hungarian National Media and Infocommunications Authority are partly accessible to the public through published annual reports, and certain transparency data are centralized at the EU level for broader public and civil society scrutiny. The NMHH's role includes facilitating transparency and public empowerment but direct full public accessibility of all detailed reports from Hungarian online service providers under the DSA to civil society watchdogs seems limited to aggregated and processed information in annual summaries and specific certifications, with granular data hosted in EU-wide platforms.

5.9 Cooperation with Other Member States and EU Bodies

Is there any formal mechanism for cooperation between your national authorities and other EU member states in enforcing these regulations?

The DSA establishes a cooperation framework that requires implementing national authorities like Hungarian National Media and Infocommunications Authority to collaborate closely with each other and the European Commission to ensure consistent enforcement of the DSA across the EU. This cooperation includes exchanging information, assisting other implementing national authorities in investigations, joint enforcement actions, and participating in coordination groups at the EU level to address cross-border issues related to online service providers.

While the Hungarian National Media and Infocommunications Authority is formally part of this EU-wide cooperation framework mandated by the DSA, there have been political concerns raised at the EU level about the NMHH's independence in enforcing the DSA, which somewhat clouds the perception of its cooperation role. Nevertheless, under the DSA legal framework, the Authority is expected to actively cooperate with other national authorities within this structured network for enforcement purposes.

How do EU-level entities (e.g., the European Commission, Europol) coordinate or facilitate the exchange of best practices?

The framework established by the DSA includes the Digital Services Coordinators (DSCs) from each EU Member State who are responsible for monitoring and enforcing the regulation nationally. The European Commission works closely with these DSCs to ensure consistent enforcement across the EU. The Commission organizes regular meetings and cooperation platforms where DSCs and other relevant national authorities share experiences, best practices, and challenges. This fosters harmonized application and enforcement of the DSA across member states. Technical support, guidelines, toolkits, and training is also provided to authorities to build enforcement capacity and improve regulatory practices.

Apart from this, the European Board for Digital Services, established under the DSA, serves as an EU-level body facilitating cooperation, streamlining information exchange, and ensuring policy coherence among DSCs and the Commission. As regard systemic risks and enforcement on very large online platforms, the Commission has exclusive monitoring powers but coordinates with national authorities to complement enforcement efforts.

Entities like Europol are involved when illegal content intersects with criminal investigations, enabling law enforcement cooperation on matters such as serious cybercrime and terrorism-related content aligned with the DSA framework.

Through these mechanisms, EU-level institutions ensure continuous coordination and exchange of knowledge, helping shape effective, harmonized governance of digital services across the Single Market. digital-strategy.

Have there been cross-border cases that required joint enforcement efforts?

There have been no publicly reported cross-border cases under the Digital Services Act (DSA) that required joint enforcement efforts specifically involving the Hungarian Media and Infocommunications Authority. No mentions of joint enforcement actions or cross-border investigations led by the Authority were noted. Most activities involved forwarding complaints

and cooperating with other member states' authorities, rather than direct joint enforcement efforts initiated by Hungary.

5.10 Impact on Freedom of Expression and Privacy

Have concerns been raised that the fast removal requirements under Regulation (EU) 2021/784 might lead to over-removal or censorship?

The Hungarian government has expressed apprehension about the potential disproportionate impact on freedom of expression, emphasizing that the deletion of illegal content should respect the right to free expression. There are also worries about the use of algorithms and artificial intelligence in content moderation leading to opaque decisions and the removal of legally protected speech: https://constitutionaldiscourse.com/the-unintended-consequences-of-european-content-removal-laws-on-free-expression/

Moreover, Hungarian reports indicate a significant impact of automated content moderation by platforms like Facebook and YouTube on Hungarian users, with many posts deleted and accounts suspended based on platform rules enforced by AI, often without transparent explanations or effective appeal mechanisms. The risk of over-removal is particularly linked to the trusted flagger system under the DSA, where flags from trusted organizations may lead to rapid removal of content with limited platform review, raising fears of excessive censorship and limits to freedom of expression.

Under the DSA, how are fundamental rights—such as freedom of expression and data protection—safeguarded in your national implementation?

Act CIV of 2023. safeguards fundamental rights such as freedom of expression and data protection by embedding key principles of the DSA into national law. This includes provisions ensuring that any content removal or restriction respects the right to freedom of expression, complying with EU standards and the Charter of Fundamental Rights of the European Union.

Hungary's legal framework mandates transparency from digital service providers about their content moderation practices, user rights for redress and complaint mechanisms, and safeguards against arbitrary removal of content. The law emphasizes the need for balanced enforcement that avoids

over-removal, ensuring that actions against illegal content do not unduly infringe on lawful speech. Data protection is preserved through strict adherence to the General Data Protection Regulation (GDPR), with service providers required to handle personal data lawfully, fairly, and transparently when processing user content or complaints.

Furthermore, the Hungarian Media and Infocommunications Authority as the Digital Services Coordinator, operates under these frameworks to enforce the DSA while upholding fundamental rights, ensuring that enforcement actions consider proportionality and respect users' privacy rights along with freedom of expression guarantees.

What oversight or appeal mechanisms exist for content creators or users affected by removals?

In Hungary, under the (DSA) and act CIV. of 2023, content creators or users affected by content removals have several oversight and appeal mechanisms. Platforms must inform affected users about content removal decisions, reasons for removal (if legally permissible), and available redress options, ensuring users are aware of appeal mechanisms at every step.

Users must first use the platform's internal complaint and review system, which platforms are required to provide under the DSA. This process allows users to challenge content takedown or account restriction decisions directly with the platform. If the platform denies the complaint, users can seek redress by the Hungarian National Media and Infocommunications Authority. The Authority oversees digital content disputes and can review decisions related to content removal.

Users dissatisfied with the Authority's decisions may appeal these through the Hungarian courts, providing a multi-tiered judicial oversight of content moderation decisions.

After exhausting domestic remedies, users can escalate cases to the Appeals Centre Europe (ACE), an independent supranational dispute resolution body certified to handle content moderation disputes under the DSA. ACE offers an independent review by digital rights experts and issues non-binding resolutions that platforms must justify if ignored.

5.11 Comparisons with Other Jurisdictions

If relevant, do lawmakers or regulators reference how other EU member states are implementing these regulations?

Hungarian public debate and policymaking show awareness of diverse DSA implementation approaches across the EU, partly sparked by scrutiny and criticism from EU institutions and independent organizations regarding Hungary's own regulatory steps. Hungary's higher public awareness of the DSA compared to many other member states reflects this engagement with the broader European context. Hungarian discussions often consider the balance between enforcing EU digital rules and addressing national sovereignty concerns, while observing how other countries handle freedom of expression, transparency, and platform accountability under the DSA.

Additionally, Hungary's designation of the Hungarian Media and Infocommunications Authority as the Digital Services Coordinator aligns with EU-wide enforcement structures, and there is reference to similar roles and frameworks in other states. This comparative outlook is part of ongoing conversations about harmonization challenges, enforcement cooperation, and the political context of implementing the DSA across varying national environments within the EU.

Are there notable differences in how your country addresses terrorist content or digital services obligations compared to neighboring states?

Hungary has implemented the DSA within a context marked by strong governmental control over media and digital platforms, with institutions like the Hungarian Media and Infocommunications Authority involved in enforcement but concerns have been formulated regarding its political independence. In contrast, many neighboring states maintain regulatory bodies with more independence and enforce DSA obligations with a clearer emphasis on upholding freedom of expression and democratic values in line with EU policy goals. Hungary's strategic prioritization of national sovereignty and governance of digital spaces differs from neighbors that promote more cooperative enforcement frameworks under the DSA.

6
THE ROLE OF THE ADMINISTRATOR OF THE NATIONAL TOP-LEVEL DOMAIN (.CZ/.SK/.PL/.HU)

6.1 Institutional Setup and Governance

Which entity (public, private, or non-profit) administers the national top-level domain (TLD) in your country?
The national top-level domain (TLD) for Hungary is the .hu domain. It is administered by the Council of Hungarian Internet Providers, a non-profit entity. The central registry for the .hu domains, called the Registry, is operated by ISZT Nonprofit Kft., a subsidiary of the Council of Hungarian Internet Providers (CHIP). The Council is responsible for regulating the .hu ccTLD based on a contract with ICANN. The Registry (ISZT Nonprofit Kft.) handles domain name registration records and operates the Hungarian central name servers, while registrars serve domain applicants and registrants.

How is this administrator selected or designated (e.g., through a government contract, regulatory framework, or historical precedent)?

The administrator of the Hungarian top-level domain (.hu) is designated through a system of self-regulation established by the Scientific Association of the Council of Hungarian Internet Providers (CHIP). This association created the Domain Registration Rules and Procedures under the framework provided by Section 15/A of Act CVIII of 2001. These rules form part of a contractual and regulatory system ensuring the uniform delegation, registration, and maintenance of .hu domain names.

What legal or regulatory instruments define and govern the role of this TLD administrator?

The role of the Hungarian top-level domain (.hu) administrator is defined and governed primarily by the following legal and regulatory instruments:

Act CVIII of 2001, Section 15/A: This provision of Hungarian law enables the possibility of self-regulation for internet service providers, under which the

Scientific Association of Hungarian Internet Providers Council (CHIP) establishes domain registration rules and procedures.

Domain Registration Rules and Procedures are established by the Scientific Association of Hungarian Internet Providers Council (CHIP) based on the self-regulation framework in Act CVIII of 2001. These rules form the contractual system governing the delegation, registration, maintenance, and dispute resolution of .hu domain names.

Furthermore, a detailed domain Registration Policy complements the rules, specifying terms for application, registration, maintenance, cancellation, suspension, revocation, transfer of domain names, and legal dispute resolution.

These instruments collectively provide the self-regulatory framework that governs the administration of the .hu domain, ensuring uniformity, safeguarding registrants' rights, and establishing legal responsibilities for domain applicants and registrants.

6.2 Responsibilities and Mandate

What are the core functions of the TLD administrator (e.g., domain name registration, policy enforcement, dispute resolution)?

The first task of the Hungarian top level domain administrator is the domain name registration: The Registry registers and keeps records of .hu domain names, granting the right of use (delegation) of a domain to the registrant through authorized registrars. Applicants apply via registrars, who handle customer service and maintenance contracts with registrants.

Secondly, the Council of Hungarian Internet Providers regulates the .hu ccTLD, setting policies such as the domain registration policy, maintaining uniform order of registration, delegation, and maintenance of domain names, and protecting the rights of registrants and others.

Thirdly, the administrator operates the registry; the central name servers and databases for .hu domains to ensure accessibility and updates.

Fourthly, there is an Alternative Dispute Resolution Forum independent of the Registry and registrars that handles legal disputes relating to domain registration under the domain registration policy and procedural rules.

Does the administrator have any responsibilities related to content regulation or oversight of hosted websites?

The Hungarian Top Level Domain administrator does not have responsibilities related to content regulation or oversight of hosted websites. Their duties are limited to domain name registration, policy enforcement related to domain names, maintenance of the domain registry, and legal dispute resolution.

Specifically, liability for the content and use of the domain names lies exclusively with the domain applicants and registrants. The domain name registration policies prohibit domain names that are illegal, shocking, horrifying, or delusive, but there is no indication that the administrator regulates or monitors the actual content hosted on websites under .hu domains. Content regulation in Hungary is covered by other laws and regulatory bodies, not the domain administrator.

6.3 Registration Policies

What rules or policies govern the registration of domain names under the national TLD (e.g., residency requirements, trademark considerations)?

The registration of .hu domain names in Hungary is governed by a detailed Domain Registration Policy which includes the following key rules and policies:

There are no strict residency requirements for registrants. Both individuals and legal entities inside and outside Hungary can register .hu domain names. However, Hungarian entities and residents are generally preferred and certain domain categories may have specific residency or presence requirements.

Registrants must ensure that the domain name does not infringe on third party trademarks or rights. The policy prohibits registering domain names that violate trademark laws, are confusingly similar to well-known trademarks, or are abusive registrations.

Domain names must conform to technical and format specifications, avoid illegal or offensive content, and comply with the policy prohibiting domain names that are misleading, unlawful, or violate public order.

Domain names must be applied through accredited registrars who verify compliance with policies and handle registrations.

In cases of conflicts involving domain name rights (e.g., trademark conflicts), a domain dispute resolution process is in place to resolve claims based on the registration policy.

Are there restrictions or special requirements for certain types of domain names (e.g., government domains, restricted sectors)?

.hu domain names must be between 2 and 63 characters long (fewer if using accented Hungarian characters). Allowed characters include lowercase Latin letters a-z, specific Hungarian accented lowercase letters, numbers 0-9, and hyphens with certain placement restrictions (e.g., cannot begin or end with a hyphen or have two consecutive hyphens in the third and fourth positions).

Certain restricted domain names exist under subdomains such as .gov.hu for government use. Similarly, second-level domains like .co.hu, .info.hu, .org.hu, .shop.hu, etc., have sector-specific restrictions and eligibility requirements.

Although registrations are generally open, some domains, especially restricted or official ones, may require local presence or additional documentation.

Domain names must not violate trademark laws, infringe rights, or be misleading or illegal.

Does the administrator have a public policy document or guidelines outlining registration procedures and dispute resolution processes?

The Hungarian top level domain administrator provides a public policy document called the "Domain Registration Policy," which outlines the registration procedures and dispute resolution processes.

The policy document is issued by the Scientific Association of the Hungarian Council of Internet Providers following legal provisions (Act CVIII of 2001). The policy covers definitions, application and registration rules, domain name maintenance, termination, technical requirements, administrative contacts, and legal dispute settlement procedures. The dispute resolution sections detail procedures for settling legal disputes both prior to and after domain delegation. The policy is available in Hungarian and English, with the Hungarian version prevailing in legal interpretation. The policy is part of the contractual system for managing .hu domains and ensures rights protection and uniform registration order.

Hungarian: https://www.domain.hu/domainregisztracios-szabalyzat/

English: https://www.domain.hu/domain-registration-policy/

6.4 Dispute Enforcement

Under what circumstances can the administrator revoke or suspend a domain name?

The Hungarian top level domain administrator can revoke or suspend a domain name under several circumstances:

The registrant waives the use of the domain with a valid declaration or authentic instrument.

A legal person's registration application has been finally rejected by a court or authority.

The domain maintenance contract has been terminated, and no new contract has been registered within 30 days.

Suspension is imposed for violations, and the cause of suspension is not removed within specified time frames (15-30 days depending on the case).

Registrant fails to provide or update accurate and real contact data after being requested by the Registry.

The administrative contact does not consent to the processing of their personal data, and the issue is not corrected.

The domain registration lacks an application or maintenance contract or necessary declarations.

A final court or public authority decision orders the registration or use of the domain name be deemed unlawful or deleted.

The decision of the Alternative Dispute Resolution (ADR) Forum mandates revocation, and the registrant fails to appeal or contest the decision within 30 days.

Following revocation, the domain is deleted and becomes freely available after a moratorium of 60 days, with some rights reserved for prior registrants or legal successors during that period. domain

6.5 Collaboration with Government and Law Enforcement

Does the TLD administrator coordinate with government agencies or law enforcement in addressing illegal online activities (e.g., court orders to suspend domains)?

The Hungarian top level domain administrator coordinates indirectly with government agencies and law enforcement in addressing illegal online activities primarily through legal and administrative mechanisms.

The domain registration policy allows for domain suspension or revocation following a final court or authority decision, including court orders to suspend domains involved in illegal activities.

Domains under the special government .gov.hu domain are managed separately by the state organization NISZ Zrt., ensuring government control for official state-related domain names.

The alternative dispute resolution and legal dispute settlement mechanisms enable authorities to resolve domain-related conflicts based on legal rulings.

Are there formal procedures or agreements (memoranda of understanding) in place to facilitate this cooperation?

No such procedure or memorandum of understanding exist.

Have there been notable cases in which the TLD administrator took action against domain owners at the government's request?

No such case has been registered.

6.6 Transparency and Accountability

Are domain holders or the public able to appeal or challenge decisions made by the TLD administrator?

Yes, domain holders and the public in Hungary are able to appeal or challenge decisions made by the Hungarian top-level domain administrator through a formal dispute resolution process. The Scientific Association of the Hungarian Internet Service Providers Council operates an Alternative Dispute Resolution Forum (ADRF) which provides out-of-court settlement of disputes related to domain applications, registrations, and use. This forum is independent of the registry and registrars and handles complaints electronically via an Integrated Complaints Handling System.

Complaints can be submitted if a domain application is rejected or if a registered domain is alleged to infringe on legitimate rights. The ADRF can decide to revoke or transfer domain names based on rights recognized under national or EU law. Decisions by the ADRF can be challenged before state courts, and court proceedings can suspend the implementation of ADRF rulings. The forum functions as a first-instance adjudicatory body, and parties may still have the option to refer disputes to arbitration or court.

6.7 Economic and Market Considerations

Are registration fees or other costs regulated by the government, or set independently by the TLD administrator?

The registration fees and other costs for Hungarian top-level domain (.hu) names are set by the domain administrator, ISZT Nonprofit Kft., operating under the Scientific Association of the Hungarian Internet Providers Council. The Domain Registration Policy, which governs the registration process, is a self-regulatory framework established by the association rather than direct government regulation over fees.

The fees for registration, renewal, and other services are determined contractually between registrants and registrars, who pay fees to the registry (ISZT). The policy does not specify government-fixed fee rates; instead, fees are part of the operational management by the domain administrator under the self-regulation framework. Public references show typical fees such as €29 for 2 years registration, €15 annual renewal, and minor fees for domain transfer, indicating market-driven pricing within the regulatory terms.

7
INDEPENDENT OVERSIGHT MECHANISMS

The role of ombudsman institutions, national human rights bodies, and other watchdogs

7.1 Institutional Mandates and Legal Foundations

Which institutions in your country serve as independent oversight mechanisms, such as ombudsman offices or national human rights commissions?

Hungary has several institutions serving as independent oversight mechanisms, primarily centered around the Commissioner for Fundamental Rights (Alapvető Jogok Biztosa), commonly known as the Ombudsman, serving as Hungary's main independent oversight body and National Human Rights Institution (NHRI). This institution operates independently from other state agencies and reports only to Parliament.

Under what legal or constitutional provisions are these institutions established, and how is their independence safeguarded?

Hungary's oversight institutions are established through constitutional and statutory provisions with formal independence safeguards, though their practical effectiveness faces political constraints.

Article 30 of the Fundamental Law (2011) establishes the Commissioner for Fundamental Rights as the primary oversight institution. This constitutional provision mandates that the Commissioner "shall perform fundamental rights protection activities" and grants authority to investigate violations by public authorities. Act CXI of 2011 on the Commissioner for Fundamental Rights provides comprehensive regulatory framework. This statute details the Commissioner's mandate, including special attention to children's rights, minority rights, vulnerable social groups, and future generations' interests. The Commissioner is nominated by the President and elected by Parliament for six-year terms, providing stability beyond electoral cycles. Any Hungarian citizen with a law degree may be elected, subject to parliamentary approval. The Commissioner and deputy commissioners enjoy full parliamentary immunity, including immunity from prosecution and inviolability protections, unless Parliament suspends such

immunity. They cannot be held liable for opinions expressed in official capacity. The Commissioner operates independently in procedures, is "only subject to the law," and cannot receive instructions from other authorities. The institution reports exclusively to Parliament, not the executive branch. The Commissioner's budget is allocated through parliamentary appropriations, providing some insulation from executive control. The effectiveness of these safeguards ultimately depends on political will for compliance, as the Commissioner lacks enforcement powers and relies on moral authority.

Do their mandates explicitly cover digital rights, freedom of expression online, or the regulation of online content?

The Commissioner's mandate effectively covers digital rights through general fundamental rights provisions rather than specific digital mandates.

7.2 Scope of Authority and Responsibilities

What types of complaints or issues can be brought to these oversight bodies (e.g., alleged censorship, violations of online privacy, hate speech)?

The Commissioner for Fundamental Rights accepts complaints regarding any fundamental rights violation by public authorities.

Do these institutions have the power to issue legally binding decisions, recommendations, or only advisory opinions?

The Hungarian Commissioner for Fundamental Rights does not have the power to issue legally binding decisions. The institution operates primarily through recommendations and advisory opinions rather than enforceable sanctions. This limitation significantly affects the Commissioner's effectiveness in addressing systemic issues like hate speech under-enforcement or digital rights violations.

How do they prioritize or select cases related to digital rights or internet regulation?

Based on available information, the Hungarian Commissioner for Fundamental Rights does not appear to have explicit public criteria for prioritizing digital rights or internet regulation cases. The Commissioner accepts complaints free of charge through multiple channels (oral, written, email, online platform) and has broad authority to investigate fundamental rights violations by public authorities.

However, there is no publicly documented prioritization framework specifically for digital rights cases. Unlike some other ombudsman institutions, Hungary's Commissioner does not publish detailed case statistics.

7.3 Complaints and Redress Mechanisms

How can citizens, NGOs or persons affected file complaints regarding internet-related grievances (e.g., blocked websites, content takedowns)?

The Internet Hotline of the National Media and Infocommunications Authority investigates online abuses including illegal content, content harmful to minors, or wrongful content takedowns. Complaints can be submitted online via a dedicated form or by email (internethotline@internethotline.hu). Reporting can be anonymous but providing contact details allows follow-up. The Hotline will check if the online platform has its own complaint procedure and may contact the platform if direct reporting was unsuccessful. If the case involves potential criminal offenses, it will be forwarded to the investigating authority promptly.

The Online Platform Dispute Resolution Council was established as an alternative out-of-court dispute resolution forum under the EU Digital Services Act (DSA) This body handles disputes related to harmful platform decisions like content removal or profile blocking; submissions Require a written complaint submission, a procedural fee of HUF 3,000, and details about the applicant, service provider, and complaint facts. The aim is to provide efficient dispute resolution without court involvement.

Council of Hungarian Internet Providers (ISzT) handles complaints concerning domain name registration or usage disputes via an Alternative Dispute Resolution Forum. Other complaints related to dissatisfaction with registrars, the Registry, or dispute resolution outcomes are handled through the ISzT's Integrated Complaint Handling System. domain

The Hungarian Competition Authority accepts complaints about unfair practices including those related to internet services. Complaint submission is free and can be done using Competition Authority's form. The Authority may initiate proceedings based on complaints without making the

complainant a party unless proceeding is initiated. Complaints can be anonymous to the undertakings involved.

Apart from this, NGOs like Transparency International Hungary handle complaints about their conduct but also provide guidance on complaint procedures to the public.

Data protection complaints can be filed with the Hungarian Data Protection Authority for issues related to personal data misuse online.

Consumer and e-commerce-related online disputes can be resolved through platforms like the Hungarian Financial Arbitration Board.

Are these processes user-friendly, accessible online, or free of charge?

The National Media and Infocommunications Authority's Internet Hotline offers an online complaint form and email submission, making it easy for users to report internet issues such as blocked websites or harmful content. The Hotline is reported to send timely feedback and to reach out to platforms when users do not get responses, which enhances usability.

The Council of Hungarian Internet Providers manages complaints via an Integrated Complaint Handling System online. Users can file both domain-related disputes and simpler claims through this system.

The Online Platform Dispute Resolution Council provides an alternative dispute resolution channel with a formal written complaint process. However, it requires clear documentation and a small procedural fee of 3000 HUF (8-9 USD) to cover administrative costs.

The Hungarian Competition Authority accepts complaints through an online form with mandatory fields to complete for submission.

What remedies (e.g., compensation, policy recommendations, sanctions) can these institutions provide or recommend?

Internet Hotline acts as a legal advisory and mediation service. It helps remove illegal or harmful content by investigating reports and contacting service providers to request content removal or other corrective actions. The Hotline guides users on how to act themselves and informs them of civil and

criminal liabilities relevant to the case. It does not provide direct compensation but can forward cases involving potential crimes to authorities for prosecution or further action.

Council of Hungarian Internet Providers (ISzT) domain disputes under an Alternative Dispute Resolution Forum, which is an out-of-court mechanism. It resolves disputes about domain registration and use, issuing binding decisions in these cases. The ISzT also investigates and responds to complaints about registrars or registries. It facilitates resolution and enforces domain-related policies but does not award consumer compensation.

Online Platform Dispute Resolution Council provides an efficient out-of-court settlement forum for disputes like content takedown or account suspension. Resolutions here can include reinstatement of content or accounts but generally do not involve financial compensation.

Hungarian Competition Authority can investigate and impose sanctions, including fines, on companies violating consumer rights or competition laws, including online practices. Since March 2024, it has authority to temporarily disable access to electronic data or shut down websites in cases of serious breaches. This authority provides powerful sanctions to compel compliance but not direct individual compensation.

7.4 Interaction with Government and Legislators

Are ombudsman or human rights bodies consulted during the legislative process on laws affecting internet governance or digital rights?

The Commissioner for Fundamental Rights (the Hungarian Ombudsman) and other national human rights institutions are involved in consultations on media and internet freedom legislation. For example, in early 2021, consultations took place with various Hungarian authorities including the Commissioner for Fundamental Rights on freedom of expression and media legislation, highlighting the Ombudsman's participation in discussions influencing legislative developments affecting digital rights.

Do they issue formal opinions or recommendations to government entities, and are these taken into account?

The Hungarian Ombudsman frequently reviews government and public authority actions regarding fundamental rights and social inclusion. It makes numerous formal recommendations seeking remedy for identified constitutional improprieties, policy gaps, or misapplications of law. Over half of these recommendations have been promptly accepted by state organs, with only a small minority contested. The Ombudsman also engages in professional dialogues aimed at reaching consensus and sometimes initiates constitutional court cases to enforce rights. ias.

Have their recommendations ever led to significant changes in internet-related legislation or regulation?

No significant changes have been reported in internet-related Hungarian legislation or regulation which would have been initiated by recommendations from the Hungarian ombudsman or human rights organizations.

7.5 Case Studies and Notable Interventions

Can you provide examples of significant cases where these institutions intervened to address online censorship, disinformation, or hate speech?

One key case involved the European Court of Human Rights (ECtHR) ruling against Hungary concerning liability for online comments. The case Magyar Tartalomszolgáltatók Egyesülete (MTE) versus Hungary dealt with platform liability for user comments, online freedom of expression, and the context in which comments appeared. The ECtHR found that excessive liability standards imposed by Hungarian courts violated freedom of expression, especially noting the internet's characteristic of lower register and provocative speech. This ruling aimed to mitigate earlier strict liability decisions (like the Delfi case) and softened Hungary's approach to online platform responsibility for user-generated content.

Another example of media freedom concerns arose with Hungary's 2011 new media law that granted the government extensive powers to control the internet and media, including registration requirements and content control

such as censorship of hate speech or offensive content. This law sparked protests and critiques from human rights organizations due to threats to freedom of speech and internet freedom.

Additional instances focus on surveillance and attacks on journalists connected to digital rights and censorship issues. For example, the use of Pegasus spyware against journalists raised demands from media freedom defenders for investigations and safeguards.

Were their interventions successful, and did they lead to policy changes, legal reforms, or compensation for victims?

Some partial successes have been experienced, however, systemic challenges have remained.

What challenges did they face (e.g., resistance from governmental bodies, lack of cooperation from digital platforms)?

Resistance from governmental bodies has been strong. The government consolidated control over the telecommunications and media landscape, deploying spyware such as Pegasus to surveil journalists, lawyers, and political opponents. This atmosphere of surveillance, along with the classification of surveillance data as state secrets, severely limits transparency and redress possibilities, making it difficult for ombudsmen and NGOs to uncover abuses and advocate for victims effectively.

There have been legal and institutional pressures. For example, the termination of the mandate of Hungary's Data Protection Ombudsman was ruled by the Court of Justice of the EU as non-compliant with EU law, yet Hungary had not implemented the required changes or rectified these issues. This signals a lack of cooperation and compliance with supranational legal standards, hindering effective rights protection.

Political and legal environments have limited independence. The Hungarian media and digital regulatory authorities are often seen as lacking independence from government influence, creating obstacles for fair investigation and effective advocacy against censorship or restrictions.

Human rights organizations also face difficulties with digital platforms. Platforms sometimes apply censorship inconsistently or lack transparency

in content moderation, complicating efforts to challenge wrongful removals or restrictions. Moreover, international cooperation is required to tackle cross-border issues like spyware abuse or data protection violations, which adds complexity to interventions.

These challenges reflect a broader context of restricted civic space, state surveillance, and hybrid authoritarian tactics in the digital realm in Hungary, complicating the work of the ombudsman and human rights defenders.

7.6 Effectiveness and Criticisms

How do stakeholders (e.g., civil society, media, academia) perceive the effectiveness of these independent oversight mechanisms in protecting online rights?

Civil society and media frequently highlight that Hungary's oversight bodies, including media regulators, lack genuine independence from the ruling party (Fidesz). This compromises their ability to protect online rights effectively. The Media Council, responsible for enforcing digital services regulations like the EU's Digital Services Act (DSA), is seen as politically controlled, undermining trust in its impartiality.

The political environment is described as exhibiting authoritarian tendencies that co-opt liberal democratic frameworks to maintain control over digital space and suppress dissent. This has resulted in an oversight landscape where EU digital rights frameworks exist on paper but cannot be fully implemented or enforced in a meaningful way domestically.

Academia and media experts emphasize that Hungary's approach to digital sovereignty often conflicts with principles of freedom of expression, pluralism, and privacy. This creates deep skepticism about the ability of existing oversight mechanisms to protect online rights, especially given the government's use of disinformation and control over media narratives.

Many NGOs and civil society actors view recent laws and institutional changes—like the 2023 Sovereignty Protection Act and related bills targeting foreign-funded organizations and independent media—as further eroding civic space and hindering the effective functioning of oversight bodies. These

laws have drawn criticism from the European Commission and human rights watchdogs for violating fundamental rights.

Have there been criticisms or concerns regarding their impartiality, resources, or scope?

The Media Council has been widely criticized for its lack of independence from the government, with many stakeholders describing its decisions as politically motivated and biased in favor of pro-government media outlets. Independent media frequencies have been canceled or not renewed, while tenders tend to favor outlets aligned with the ruling party, which distorts media pluralism.

The regulatory body's composition and decision-making process have been described as discriminatory and non-transparent, undermining basic principles of the rule of law. This includes blocking mergers involving independent media while facilitating those involving pro-government media, contributing to a highly concentrated media market under government influence.

There are concerns about the lack of meaningful legal safeguards to secure the independence of media oversight. This structural weakness leads to a regulatory environment where the Media Council can exert heavy-handed control, effectively silencing dissenting voices and reducing media freedom.

The resources and scope of oversight mechanisms are limited by political interference and systemic capture. This has rendered them insufficient to challenge government control or protect independent voices effectively. Moreover, recent legislative proposals pose further threats by enabling financial restrictions or blacklisting of independent media and civil society organizations receiving foreign funding.

Do they face budgetary or political constraints that limit their ability to address digital rights issues effectively?

Independent media outlets and organizations working on digital rights heavily rely on foreign funding and grants, especially from international donors like the U.S. and the EU. However, recent cuts in foreign funding and government campaigns to restrict access to these funds through legislation

create severe financial uncertainty for these actors, threatening their survival and capacity to operate effectively.

The Hungarian government has introduced laws, such as the Sovereignty Protection Office's blacklist and related tax laws, which severely restrict foreign funding to NGOs and media organizations flagged by the government. Violations can lead to huge fines or organization dissolution, creating a chilling effect that hampers independent voices from receiving necessary financial resources.

Political influence strongly constrains oversight mechanisms, including regulatory agencies and watchdogs, many of which lack institutional independence. This political pressure undermines their ability to address digital rights issues such as censorship, disinformation, and hate speech adequately.

7.7 Future Outlook and Reform

Are there ongoing discussions about reforming or expanding the mandates of these institutions to better address internet governance and digital rights challenges?

A major recent legislative proposal, the Bill on the Transparency of Public Life submitted by the ruling Fidesz party, would grant broad powers to the Sovereignty Protection Office (SPO) to blacklist media outlets and civil society organizations receiving foreign funding. This bill aims to restrict foreign influence but essentially targets independent media and NGOs, potentially enabling financial strangulation and closure of critical voices. This suggests a crackdown rather than expansion or reform toward greater independence or oversight capacity.

How might emerging technologies (AI, automated content moderation) influence the need for stronger or more specialized oversight?

Hungary's growing reliance on AI for real-time content moderation, as seen in classified ads and social media moderation, necessitates specialized regulatory frameworks to ensure the protection of users' rights and to maintain fairness and transparency. The EU Digital Services Act (DSA) and the AI Act set new standards for content moderation, emphasizing the

requirement for transparency, supervision, and human oversight on high-risk AI systems, which include automated moderation. These regulations are likely to influence Hungary's approach to AI oversight, balancing the efficiency gains of AI with the crucial role of human moderators in understanding cultural and contextual nuances.

Moreover, given the rapid advancements and adoption in AI, Hungary faces the dual challenge of protecting fundamental rights such as freedom of expression and privacy while ensuring that AI moderation tools are accurate and not misused to manipulate public opinion or unfairly restrict lawful content. Specialized oversight mechanisms will be needed to implement the EU regulations effectively and manage the complexity introduced by automated AI systems.

Are there proposals to create new institutions or strengthen existing ones to address the complexities of the digital environment?

Hungary has made recent legislative efforts to strengthen and unify oversight in the digital environment, particularly through the 2024 Cybersecurity Act (act LXIX. of 2024). This Act, which entered into force on January 1, 2025, consolidates Hungary's cybersecurity legal framework, repealing earlier fragmented laws and providing a more robust and unified regulatory approach. It addresses the implementation of the EU NIS2 Directive and sets clear obligations for entities in both the public and private sectors regarding cybersecurity measures.

The supervisory authority for regulated activities plays a central role in implementing these regulations, overseeing registrations, audits, and compliance. The Act also designates the Special Service for National Security as the national cybersecurity authority for certain critical public administration bodies and important state-owned enterprises. This marks a strengthening of Hungary's institutional capacity to oversee cybersecurity, reflecting the complexities of the contemporary digital environment.

There are also specific regulatory frameworks for mandatory security audits, incident reporting, and cooperation between national and international cybersecurity entities. These measures indicate a move

toward more specialized and formalized oversight institutions in response to digital challenges.

While the focus is on cybersecurity, these efforts complement the broader need for oversight in related areas like AI and automated content moderation, emphasizing the development of institutional capacities to handle new technological risks.

7.8 Comparisons and Best Practices

Do your country's oversight bodies benchmark against international best practices or models from other jurisdictions?

Hungary's internet oversight bodies do benchmark against international best practices and models, particularly in the realm of cybersecurity and internet security regulations. Hungary has aligned its cybersecurity legal framework with the EU's NIS2 Directive, reflecting lessons learned from prior implementation gaps. The 2024 Cybersecurity Act consolidates and strengthens Hungary's cybersecurity legislation, incorporating EU directives and harmonizing requirements with international standards. The Supervisory Authority for Regulated Activities (SZTFH) oversees compliance, including coordination with international entities. Additionally, Hungary's National Cyber Security Centre (NCSC Hungary) operates based on strong national and international cooperation to protect e-services and critical infrastructure, aligning with EU cybersecurity directives. Recent legislation like the Act LXXVIII of 2024 addresses online aggression, introducing new rules to ensure responsible online communication, again integrating international policy considerations. These measures illustrate Hungary's efforts to benchmark and adopt international best practices in internet oversight and cybersecurity.

Are there examples of pioneering or innovative approaches taken by these institutions that could be emulated elsewhere?

Key innovations include:

The 2024 Cybersecurity Act, which consolidates and harmonizes Hungary's cybersecurity legislation into a unified framework, improving upon the fragmented and incomplete 2023 Act. This approach addresses gaps in

compliance and enforcement while aligning with the EU's NIS2 Directive, providing a robust legal infrastructure for cybersecurity protection across both public and private sectors.

The establishment of the Supervisory Authority for Regulated Activities (SZTFH), which handles registrations, audits, and enforcement in a centralized and streamlined manner. The authority reviews extensive registrations and maintains a register of NIS2 auditors, enhancing oversight efficiency.

How does your country's independent oversight framework compare with regional or international standards (e.g., Council of Europe recommendations, UN guidelines)?

Hungary's independent internet oversight framework is strongly shaped by its recent comprehensive cybersecurity legislation, notably the Cybersecurity Act of 2024 that took effect on January 1, 2025. This Act consolidates previous fragmented regulations and fully transposes the EU's NIS2 Directive on cybersecurity, establishing broad supervisory powers for the Hungarian Supervisory Authority for Regulated Activities (SZTFH). The SZTFH oversees cybersecurity compliance and has enforcement powers, including inspection, audits, and sanction imposition on private sector entities considered essential or important under the law. There is also coordination with other authorities like the National Security Authority for public administration and the Ministry of Defence for defense sectors. The regulatory framework imposes obligations on organizations such as mandatory cybersecurity audits, contracts with accredited auditors, and incident reporting within strict timelines, at risk of significant fines for non-compliance.

While Hungary enjoys relatively open internet access with some content restrictions and monitoring, its independent oversight in cybersecurity is robust, formal, and rigorous, mirroring EU-wide harmonization efforts but with strong national enforcement focus.