Visegrad Alliance
for Digital Rights
and Disinformation Defense

NATIONAL REPORT

SLOVAKIA

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

ĽUBOMÍR ZLOCHA

Researcher
Slovak Academy of Sciences, Institute of State and Law

JUDr. Ľubomír Zlocha, PhD. is the author of several professional and scientific articles in the field of commercial law and civil law. In his publications he focuses mainly on unfair competition, advertising, protection of personality rights and freedom of expression. In addition to his scientific activities, he has been actively practicing law since 2012. He devotes a significant part of his law practice to providing legal services in the field of media law. He represents one of the largest publishers in Slovakia. He is a member of the Press and Digital Council of the Slovak Republic, which is the executive body of the Association for the Protection of Journalistic Ethics in the field of ethical self-regulation of journalists.

TOMÁŠ GÁBRIŠ

Researcher
Slovak Academy of Sciences, Institute of State and Law

Prof. Tomáš Gábriš is a Slovak legal scholar specializing in legal theory, history, methodology, and philosophy. His research also addresses modern technology law. He has authored ten monographs, contributed to ten textbooks, and published over 300 works. In addition to his academic career, Prof. Gábriš is a practicing attorney, a former member of the Slovak Judicial Council, and an advisor on technology law for various organizations.

ONDREJ KOBYDA

Law Student
University of Trnava, Faculty of Law

Ondrej Kobyda is a law student with prior experience as a research assistant at the Faculty of Law, where he contributed to various academic projects. He is currently working as a paralegal at the law office Attorneity Legal, assisting with legal research, drafting, and case preparation.

1
LEGISLATION AND CASE-LAW CONCERNING DISINFORMATION AND HATE SPEECH

1.1 Legal Framework and Definitions

Within the European Union, the Slovak Republic represents a space that is exceptionally vulnerable to the effects of hoaxes, propaganda, and foreign influence operations. This vulnerability is not merely hypothetical; it is quantifiable and has real consequences for democratic processes and social cohesion. Surveys repeatedly confirm a high level of belief in conspiracy theories and disinformation narratives. According to data from 2022, up to 54% of respondents in Slovakia believe in conspiracy theories, such as the world being controlled by secret elites.[1] This situation is amplified by a widespread sense of threat from external actors, whether it be liberal democracy, Western societies, or migrants. The historical narrative of an oppressed nation further deepens distrust in institutions and creates fertile ground for alternative explanations of reality. Since 2022, Slovakia has become a focal point for influence operations with an intensity it has never faced before.

The latest quantitative surveys from 2024 and 2025 refine these findings and provide a more detailed look at the structure of this vulnerability. According to a survey by the NMS Market Research Slovakia agency, conducted in July 2025, a total of 37% of the Slovak population tends to believe hoaxes and alternative theories. This susceptible part of the population is not homogeneous but is divided into three distinct segments.[2]

Table - Distribution of the Slovak Population by Susceptibility to Believing Disinformation (July 2025)

Category	**Share in Population**	**Characteristic (Belief in Number of Theories)**
Do not believe hoaxes	63 %	Believe 0-1 of 8 presented theories
Susceptible to believing	19 %	Believe 2-3 theories
Gullible	11 %	Believe 4-5 theories
Strong adherents	8 %	Believe 6 or more theories

Source - NMS Market Research Slovakia, 2025

This data is crucial for the application of the proportionality principle in legal regulation. While the original figure (54%) suggested a majority problem, the new data (37%, with an 8% core) shows that it is a problem of a significant but clearly definable minority.

[1] Hajdu, Dominika – Klingová, Katarína – Kazaz, Jana – Kortiš, Michal (2022): GLOBSEC Trends 2022: Väčšina ľudí na Slovensku stále verí konšpiráciám a cíti sa ohrozene. *Globsec*. (online). (cited 2025-09-05). Available at : https://www.globsec.org/what-we-do/press-releases/globsec-trends-2022-vacsina-ludi-na-slovensku-stale-veri-konspiraciam

[2] Viac ako tretina populácie má sklony veriť hoaxom - NMS Market Research, (cited 2025-09-05). Available at: https -//nms.global/sk/tretina-populacie-ma-sklony-verit-hoaxom-najviac-im-veria-volici-republiky-a-smeru/

The NMS survey revealed that hoaxes are more often believed by those who are also the most convinced that they can distinguish a hoax from the truth.[3] This cognitive bias (illusory superiority) reduces the effectiveness of tools that rely on rational assessment of content by the users themselves.

However, concurrent with this vulnerability, there is a strong mandate in the population for state action. The GLOBSEC Trends 2025 survey found that up to 84% of respondents in Slovakia agree that the country should do more to combat disinformation.[4] This stance is also confirmed by CEDMO Trends data (November 2024), according to which 72% of the population perceives disinformation as a threat to Slovakia's security, and 74% agree with state restrictions on media outlets spreading disinformation.[5]

The legal framework, especially the Criminal Code (§ 361 Spreading of a false alarm, § 423 Defamation), focuses on punishing consequences. However, a deeper analysis of the causes, provided by recent psychological and sociological research, is essential to understand why these tools are often ineffective in practice. Research by the Centre of Social and Psychological Sciences of the Slovak Academy of Sciences (CSPV SAS) identifies a three-factor model of the causes of conspiratorial beliefs:

- **Individual characteristics** - Reduced cognitive and analytical abilities, lack of scientific literacy, and specific personality traits.
- **Situational characteristics (Existential threats)** - Situations causing an acute sense of anxiety, uncertainty, and loss of control, such as the COVID-19 pandemic or the war in Ukraine.
- **Environmental characteristics (Structural factors)** - Social and institutional conditions, such as objective or subjectively perceived economic uncertainty (precarity), social inequality, and low trust in institutions (political, media, scientific).

The most significant finding of this research is the re-evaluation of causality. While cross-sectional studies suggested that poor financial situation and low institutional trust cause an inclination towards conspiracies, new longitudinal SAS data (tracking respondents over time) demonstrated a reversed, or rather, bidirectional relationship.

It shows that belief in conspiracies and pseudoscientific beliefs actively predicts and increases over time:

- **Feelings of economic anxiety** - Conspiratorial beliefs at time T1 predicted increased economic anxiety at time T2.
- **Feeling of poor financial situation** - The feeling of financial precarity turned out to be more a consequence of conspiratorial beliefs than their cause.

---

[3] Spoločnosť Archives - NMS Market Research, (cited 2025-09-05). Available at: https -//nms.global/sk/category/press-releases-sk/

[4] GLOBSEC Trends 2025, (cited 2025-09-05). Available at: https -//www.globsec.org/sites/default/files/2025-05/GLOBSEC%20Trends%202025_1.pdf

[5] CEDMO Trends - CEDMO, (cited 2025-09-05). Available at: https -//cedmohub.eu/cedmo-trends-2/

- **Institutional distrust** - Pseudoscientific and conspiratorial beliefs demonstrably predicted an increase in distrust towards political institutions (national and EU), scientists, and doctors.

This phenomenon, which SAS researchers termed the "suspicious mindset trap," has direct implications for the functioning of the rule of law. The original report describes distrust in institutions as a passive "breeding ground" based on historical narratives. However, the new research proves that it is an active, self-reinforcing cycle. Belief in disinformation actively erodes trust in institutions, which subsequently (according to the structural model) increases susceptibility to believing further disinformation. For the legal system, this means that repressive tools (police, prosecutor's office, courts) are perceived by the target group as unreliable, biased, or directly as part of the conspiracy they are fighting against. This paralyzes the effectiveness of the criminal law response.

CSPV SAS research confirms a direct link between conspiratorial beliefs and behavior relevant to criminal (§ 423, § 424) and administrative law:

- **Aggression and prejudice** - Belief in conspiracy theories about COVID-19 (e.g., about the alleged role of China) was directly linked to prejudice against Chinese, but also Italian, citizens.
- **Non-normative and unlawful behavior** - Conspiratorial beliefs were positively correlated with justifying violence and willingness to violate anti-pandemic regulations (relevant to § 361 of the Criminal Code), attacking 5G transmitters, and participating in anti-state protests.
- **Health behavior** - Belief in conspiracies negatively predicted willingness to vaccinate against COVID-19 and HPV and reduced willingness to participate in medical research.

SAS research shows that the dissemination of conspiratorial narratives (e.g., about China and the virus) functions as implicit incitement that demonstrably leads to real prejudices.

Does your national legal framework define disinformation?

Slovak law does not provide a clear or universally accepted legal definition of "disinformation." However, certain types of harmful content – such as false information (e.g. hoaxes) capable of endangering public health or national security – may fall under criminal or administrative regulation.[6] The Constitutional Court of the Slovak Republic, in its decision III. ÚS 288/2017, distinguishes between disinformation and falsehoods. In its decision PL. ÚS 26/2019 concerning a moratorium on the publication of public opinion polls, a distinction is made between disinformation and purposeful information. In this decision, the Constitutional Court also points to the absence of a legal definition of disinformation.

[6] See dissemination of false alarming news (Section 361 of the Criminal Code).

Does your national legal framework define hate speech?

Slovak law does not contain an explicit legal definition of "hate speech" either. It addresses such actions through criminal law provisions prohibiting incitement to hatred, defamation of a nation, race or belief, and support of extremist groups.[7]

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

Given Slovakia's legal landscape, there is no single, comprehensive legal framework explicitly defining disinformation or hate speech. This means that Slovak legislation generally does not make specific distinctions between online and offline disinformation or hate speech in terms of their core definitions. Instead of explicit definitions, Slovak law addresses these issues through various provisions in the Criminal Code and other laws, focusing on the harmful effects or content regardless of the medium.

More recently, specific measures were introduced to address online disinformation, such as the National Security Authority's power to block websites disseminating harmful content, albeit this power was subsequently limited to a great extent.

1.2 Criminal Sanctions

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

Relevant offences sanctioned in the Criminal Code of Slovakia include:

- § 361 (Spreading alarming news),
- § 421 (Establishing/supporting extremist groups),
- § 422, § 422a, § 422b, § 422d (Extremist crimes and incitement),
- § 423 (Defamation of nation, race, or belief),
- § 424 (Incitement to national, racial or ethnic hatred).

Which criminal offences address hate speech in your jurisdiction?

From among the above, the key offences include:

- § 421 – Establishing/supporting extremist groups
- § 423 – Defamation of nation, race, or belief
- § 424 – Incitement to national, racial or ethnic hatred

[7] Defamation of nation, race, and belief (Section 423); Incitement to national, racial, and ethnic hatred (Section 424) These provisions apply whether harmful speech occurs in person, in print, or online.

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

These offences typically carry a penalty of imprisonment, with duration varying by the specific crime. For instance, Section 423 of the Criminal Code specifies a penalty range of 1 to 3 years.

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

There are additionally aggravating circumstances such as: Committing the crime in a state of emergency, Crime motivated by extremist ideology or racism, Crime affecting a large audience (e.g., public broadcast or online dissemination)

Since Slovakia has faced a sharp increase in hate speech in the online space in recent years. The Ministry of Interior of the Slovak Republic is currently introducing a legislative initiative aimed at enabling a more effective fight against the spread of hatred and fear, as well as threats, ridicule, and the humiliation of individuals or social groups. The Minister announced that he will propose a new legal definition of an offence of hate speech.[8]

1.3 Administrative Offences and Civil Measures

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

Administrative law also allows for sanctions against the media and broadcasting content that violates ethical or legal standards. The Council for Media Services can impose penalties for failure to prevent or remove hateful content.

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

The penalties include fines, suspension of broadcast licenses, and imprisonment.

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

In addition, Civil law allows individuals to seek protection of personality rights (e.g., under Civil Code § 11-13), including monetary compensation for non-material harm.

[8] (2025). Pripravujeme zákon proti šíreniu nenávisti na internete inšpirovaný Nemeckom a Rakúskom. *Ministerstvo vnútra Slovenskej republiky*. (online). (cited 2025-09-05). Available at: https://www.minv.sk/?tlacove-spravy-2&sprava=pripravujeme-zakon-proti-sireniu-nenavisti-na-internete-inspirovany-nemeckom-a-rakuskom

1.4 Scope of Instruments and Enforcement

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

Key authorities which are responsible for enforcing laws on disinformation and hate speech in Slovakia are the following: Police of the Slovak Republic, Prosecutors Office, Council for Media Services, National Security Authority and the Office for Combating Organized Crime.

How do these authorities identify and investigate potential cases?

To identify and investigate potential cases, the authorities use public reports, monitoring of online platforms and they cooperate with media regulators.

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

The National Security Authority (NBÚ) is specifically authorized to temporarily block harmful online content, particularly in cases involving cybersecurity threats or hybrid information warfare. Still, there is a significant implementation gap: The NBÚ's temporary blocking competence was used only once, after the attack of Russia on Ukraine. The NBÚ lost its competence to block disinformation sites after September 2022. However, as of October 2022 the NBÚs legal power was partially restored, but without being applied in practice.

The Council for Media Services (RPMS) supervises audiovisual platforms and may impose administrative sanctions for disinformation or hate speech in broadcast and on-demand content. However, platforms frequently respond slowly or insufficiently to moderation requests, especially during elections (e.g., only half of flagged hate speech takedowns were processed).

Until august 2024, the National Unit for Combating Extremism and Cybercrime (part of National criminal agency - NAKA) was the specialized police body dealing with online hate and extremism. In august 2024, this unit was dissolved, and its competences were redistributed between the Office for Combating Organized Crime (ÚBOK), the National Anti-Drug Unit, and the Counter-Terrorism Centre.
In addition to the above, in the complex ecosystem of the media environment in Slovakia, there is a multi-level system that seeks to regulate and cultivate both online and offline spaces. This system combines legal regulation with self-regulatory initiatives created by the actors themselves in the media market. In the fight against the negative phenomena of disinformation and hate speech, not only state institutions but also self-regulatory mechanisms and civil society activities play a key role. The most important bodies and initiatives in Slovakia include the Print and Digital Council of

the Slovak Republic[9] , the Advertising Council[10] and the Code of Practice against the Spread of Disinformation[11] , supplemented by the activities of several non-governmental organizations.

The Print and Digital Council of the Slovak Republic acts as the main self-regulatory body for journalistic ethics. It brings together publishers of print and digital media who have committed themselves to complying with the Code of Ethics for Journalists. The public can contact the council with complaints about content they consider unethical, including hate speech or gross factual errors that could be part of disinformation narratives. The Print and Digital Council of the Slovak Republic assesses whether there has been a violation of the code and issues opinions. Its main goal is to improve journalism and protect the public from unethical content. Within the scope of the Optional Protocol to the Code of Ethics for Journalists on the Protection of Human Dignity, Humanity, and Minors, the Media Services Council forwards complaints/suggestions of violations of the provisions of the Media Services Act to the Association for the Protection of Journalistic Ethics as a self-regulatory body, whose executive body is the Print and Digital Council of the Slovak Republic, which oversees compliance with the Optional Protocol.

The Advertising Council is a self-regulatory body in the field of advertising. It ensures that advertising is ethical, truthful and in accordance with the Code of Ethical Principles of Advertising Practice. Although its primary focus is not directly on combating disinformation, its activities are relevant in cases where misleading or deceptive information, or even hateful elements, appear in commercial communications. The public and companies can file complaints about advertisements they consider unethical.

The Code of Practice on Disinformation is the first tool of its kind through which relevant industry players agreed on self-regulatory standards to combat disinformation in 2018. The process of revising the Code began in June 2021 and culminated in its signing and presentation on June 16, 2022. At that time, the Code was signed by 34 signatories. It includes very large platforms (YouTube, Instagram, Facebook, TikTok, Twitter, and LinkedIn) and very large online search engines (Google and Bing), but also smaller platforms (e.g., Twitch and Vimeo), research organizations (e.g., Avaaz, Globsec, Global Disinformation Index), fact-checkers (e.g. Maldita.es) and civil society organizations (e.g. Reporters Without Borders). The aim of the Code of Practice on Disinformation is to work with platforms, research organizations, and other signatories to effectively counter the spread of dangerous disinformation in the online space. As the long-standing leader of the European Regulators Group for Audiovisual Media Services working group on disinformation, the Media Services Council worked closely with all those committed to complying with the Code in its development. The Code aims to empower users, make necessary data available for research, and significantly increase the transparency of technology companies in the area of content moderation.

The fight against hate speech and disinformation would not be complete without initiatives from the third sector. There are several projects and organizations in Slovakia dedicated to fact-checking, increasing media literacy, and actively debunking hoaxes:

[9] Tlačovo-digitálna rada Slovenskej republiky. (online). (cited 2025-09-05). Available at: https://trsr.sk/
[10] Rada pre reklamu. (online). (cited 2025-09-05). Available at: https://rpr.sk/sk/
[11] Rada pre mediálne služby. (online). (cited 2025-09-05). Available at: https://rpms.sk/kodex-postupov-proti-sireniu-dezinformacii

- Hoaxy a podvody (Hoaxes and Scams) – a project that builds on the successful work of a former police team focused on combating disinformation.[12]
- demagog.sk – a platform focused on verifying statements made by politicians and public figures.[13]
- konšpirátori.sk – a project that maintains a database of websites with controversial and disinformation content, helping advertisers avoid supporting such sites.[14]

Other initiatives: Other notable projects include the Bratislava Policy Institute[15] , which analyzes information threats, the technology company Gerulata Technologies[16] , as well as educational projects such as Zvoľ si info[17], somtu[18], and Slovenskí elfovia[19] , which are active in online discussions and refute false claims.
In the absence of a legal definition of hate speech, independent institutions approach the issue through empirical monitoring. In 2023, the Slovak National Centre for Human Rights (SNCHR) published the report "Hate Language on Political Facebook Profiles".[20] This report provides methodology and specific examples of hate speech in political discourse, thereby mapping a phenomenon that the Ministry of the Interior is trying to re-capture legislatively.

In parallel, the Central European Digital Media Observatory (CEDMO) in its special briefs, analyzed disinformation narratives during key crises, such as the 2023 parliamentary elections, the 2024 presidential elections, and the attempted assassination of Prime Minister Robert Fico in May 2024.[21] These analyses identified recurring narratives aimed at delegitimizing elections, state institutions, and accusing the media or political opponents of co-responsibility for violence, thereby directly contributing to social polarization and the erosion of institutional trust.

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

Between January and May 2025, over 500 cases related to the criminal offence of "spreading alarming news" (§ 361 of the Criminal Code) were identified. Many of these cases are still under investigation.[22]

---

[12] Hoaxy a podvody. (online). (cited 2025-09-05). Available at: https://www.hoaxyapodvody.sk/
[13] Demagog.sk. (online). (cited 2025-09-05). Available at: https://demagog.sk/
[14] Konšpirátori.sk. (online). (cited 2025-09-05). Available at: https://konspiratori.sk/
[15] Bratislava Policy Institute. (online). (cited 2025-09-05). Available at: https://www.bpi.sk/
[16] Gerulata. (online). (cited 2025-09-05). Available at: https://www.gerulata.com/
[17] Zvolsi.info. (online). (cited 2025-09-05). Available at: https://zvolsi.info/sk
[18] Somtu. (online). (cited 2025-09-05). Available at: https://www.facebook.com/groups/somtu/?locale=sk_SK
[19] Slovenskí elfovia. (online). (cited 2025-09-05). Available at:https://www.facebook.com/people/Slovensk%C3%AD-elfovia/100063976065983/
[20] Untitled - Slovenské národné stredisko pre ľudské práva, (cited 2025-09-05). Available at: https://www.snslp.sk/wp-content/uploads/Nenavistny-jazyk-na-politickych-fb-profiloch-2023_web.pdf
[21] CEDMO Fact-checking Briefy - CEDMO, (cited 2025-09-05). Available at: https://cedmohub.eu/sk/overovanie-faktov/fact-checking-briefy/
[22] Štatistika kriminality v Slovenskej republike za rok 2025. *Ministerstvo vnútra Slovenskej republiky*. (online). (cited 2025-09-05). Available at: https://www.minv.sk/?statistika-kriminality-v-slovenskej-republike-za-rok-2025

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?

The most significant court decisions shaping the interpretation of disinformation or hate speech laws in Slovakia include the following:

Milan Mazurek v. Slovakia: The Supreme Court upheld conviction of a Member of Parliament for anti-Roma hate speech

Tibor Rostas case: An editor of a journal was convicted for publishing anti-Semitic narratives in his magazine

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

Both Mazurek and Rostas cases set precedents for applying hate speech laws to public figures.

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?

The courts applied the principle of proportionality in light of Article 26 of the Constitution of Slovakia and ECtHR case law. They weighed societal harm against freedom of expression, upholding restrictions of the freedom of speech when speech is abused for incitement or denial of crimes.

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?

Slovakia has faced a sharp increase in hate speech in the online space in recent years.[23] The Ministry of the Interior of the Slovak Republic is introducing a legislative initiative aimed at enabling a more effective fight against the spread of hatred and fear, as well as threats, ridicule, and the humiliation of individuals or social groups. The Minister announced that he will propose a new legal definition of an offence or a criminal act of hate speech.[24]

[23] Friedl, Matej – Dubóczi, Peter – Ružičková, Michaela (2023): Disinformation and Propaganda as a Business: Mapping the Financial and Organisational Background of Disinformation Websites in Slovakia. *ResearchGate*. (online). (cited 2025-09-05). Available at: https://www.researchgate.net/publication/383848813_Disinformation_and_Propaganda_as_a_Business_Mapping_the_Financial_and_Organisational_Background_of_Disinformation_Websites_in_Slovakia

[24] Pripravujeme zákon proti šíreniu nenávisti na internete inšpirovaný Nemeckom a Rakúskom. *Ministerstvo vnútra Slovenskej republiky*. (online). (cited 2025-09-05). Available at: https://www.minv.sk/?tlacove-spravy-2&sprava=pripravujeme-zakon-proti-sireniu-nenavisti-na-internete-inspirovany-nemeckom-a-rakuskom

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

An example is draft bills being proposed during 2023–24 (e.g., identifying online commentators, elevated fines for hate speech) which raised alarms about restrictions on legitimate expression, prompting protests.

The main reasons for the rejection of the bills likely include a general lack of political will to tackle the issue head-on, concerns that such measures could be used to stifle freedom of expression, and fears of creating a politically controlled media watchdog. The tense political climate and the heated public debate surrounding media freedom in Slovakia have made it difficult to achieve a consensus on how to regulate online content without infringing on democratic principles.

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

These proposals were met with immediate and forceful opposition. Critics, including the opposition party Progressive Slovakia (PS), decried the move as a direct assault on free speech. The PS chairman, Michal Šimečka, characterized the SNS proposals – which also included a contentious "right to correction" for media articles and the introduction of fees for information requests – as a power grab aimed at stifling criticism of the government. He argued that such measures would grant "absolute freedom of speech to government politicians and, conversely, restrict all those who criticize the government."[25]

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?

Under Slovak domestic legislation law (Media Services Act No 264/2022, in addition to EU DSA obligations), video-sharing and on-demand platforms established in Slovakia must identify and remove hate speech, disinformation, and other "harmful content" in Slovak language. They also implement age verification, ensure local-language content moderation, and provide transparency on moderation and political advertising.[26]

[25] TASR (2024): Šimečka zároveň na tlačovej konferencii uviedol, že vládni politici zneužívajú atentát na premiéra Roberta Fica (Smer-SD), aby dosiahli svoje politické ciele. *Teraz.sk*. (online). (cited 2025-09-05). Available at: https://www.teraz.sk/najnovsie/simecka-navrhy-koalicnej-sns-su-z/799613-clanok.html

[26] Act. No. 264/2022 Coll. on Media Services and on Amendments to Certain Acts (Media Services Act). (online). (cited 2025-09-05). Available at: https://www.culture.gov.sk/wp-content/uploads/2019/12/Act-No.-264_2022-Coll.-on-media-services-and-amending-certain-acts-Media-Services-Act-1.pdf

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

Slovakia thereby follows the "notice-and-action" model. Platforms are not liable for user content unless notified of illegality. Once notified—by citizens, authorities, or RPMS—they must act promptly under the Act (and EU's Digital Services Act) to remove or block the content.

Slovakia supports the principle "what is illegal offline should also be illegal online", while suggesting that the rule should apply not only to illegal content but also to goods and services offered on internet, as those should be subject to the same regulations and standards as goods and services sold in regular shops.[27]

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

Yes, enforcement examples include EU Commission meetings with Meta, Alphabet, TikTok to pressure compliance before the 2023 parliamentary elections. Platform representatives committed to improvements under DSA. A Council for Media Services audit (early 2024) found mixed results: ~50% of hate speech takedown requests removed by TikTok/Twitter, 36% by Facebook, but only 8% by YouTube.[28]

1.8 International and Regional Considerations

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

Slovakia has implemented the EU Digital Services Act (DSA) (EU 2022/2065), in force since November 2022, applicable to large platforms. Slovakia has also enacted the Media Services Act No 264/2022. However, while party to the ECHR European Convention on Human Rights, Slovakia hasn't separately ratified any UN conventions specifically on hate speech.

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

International obligations have catalyzed national reforms e.g. the DSA and EU AVMS initiated stricter transparency and moderation duties in Slovak law, formalized through the 2022 Media Services Act and updates to cybersecurity laws. ECtHR precedents guide courts balancing hate speech vs freedom of expression.

---

[27] Hendrych, Lukáš – Yar, Lucia – Szicherle, Patrik – Strzałkowski, Michał (2020): Visegrad Four want to distinguish between 'illegal' and 'harmful' content in Digital Services Act. *Visegrad.info*. (online). (cited 2025-09-05). Available at: https://visegradinfo.eu/index.php/collaborative/595-visegrad-four-want-to-distinguish-between-illegal-and-harmful-content-in-digital-services-act

[28] Scott, Mark (2023): TikTok and Meta warned over Slovakia election lies. *Politico*. (online). (cited 2025-09-05). Available at: https://www.politico.eu/article/alphabet-tiktok-meta-slovakia-election-digital-services-act/; Hartmann, Théophane (2023): 'Disinformation led by political leaders': Slovak DSA enforcement challenged. *Euractiv*. (online). (cited 2025-09-05). Available at: https://www.euractiv.com/section/tech/news/disinformation-led-by-political-leaders-slovaks-dsa-enforcement-challenged/

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

Current discussions include a proposal to define "illegal" vs. "harmful" content more clearly, aligned with DSA principles on limited platform liability and upgrades to content-blocking standards in Cybersecurity Act to meet EU hybrid-threat obligations.[29]

1.9 Practical Challenges and Enforcement Gaps

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

There is a significant implementation gap: The NBÚ's temporary blocking competence was used only for a short while, and legislative updates have been delayed, leaving enforcement in limbo. In addition, platforms frequently respond slowly or insufficiently to moderation requests, especially during elections (e.g., only half of flagged hate speech takedowns processed).

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

Yes, an example of under-enforcement is that the NBÚ lost legal power to block disinformation sites after September 2022 pending new legislation. However, as of October 2022 the NBÚs legal power was restored in a different form. Still, this competence is not being used currently.[30]

Additionally, while authorities forwarded deletion requests before the 2023 election, Telegram refused to comply, exploiting a regulatory exemption.

[29] Hendrych, Lukáš – Yar, Lucia – Szicherle, Patrik – Strzałkowski, Michał (2020): Visegrad Four want to distinguish between 'illegal' and 'harmful' content in Digital Services Act. *Visegrad.info*. (online). (cited 2025-09-05). Available at: https://visegradinfo.eu/index.php/collaborative/595-visegrad-four-want-to-distinguish-between-illegal-and-harmful-content-in-digital-services-act; Sokol, Pavol – Bachňáková Rózenfeldová, Laura (2025): Content blocking mechanism in cybersecurity: Slovakia case study. *SpringerOpen*. (online). (cited 2025-09-05). Available at: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-025-00190-x#Sec7

[30] (2022): Slovakia loses power to block disinformation websites. *The Slovak spectator*. (online). (cited 2025-09-05). Available at: https://spectator.sme.sk/politics-and-society/c/slovakia-loses-power-to-block-disinformation-websites

2
ROLE OF AUTOMATIZATION AND AI IN CONTENT REGULATION

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

Two days ahead of the 2023 parliamentary elections, a falsified audio clip appeared online. It falsely depicted a conversation between Progressive Slovakia (political party) leader Michal Šimečka and journalist Monika Tódová, discussing vote-rigging and allegedly buying votes from the Roma community. Fact-checking by AFP and others confirmed AI-generated signs. This deepfake was created using AI tools (e.g., Eleven Labs) and was shared during Slovakia's legally mandated 48-hour election silence. However, no legal tools were available to prevent this situation and its misuse in the election process. The Slovak Republic's approach to regulating artificial intelligence (AI) and automated content moderation is thus clearly characterized by a significant gap between the rapid evolution of technology and the more deliberate pace of legislative adaptation. This "regulatory lag" has left the nation reliant on forthcoming European-wide legal frameworks, creating a temporary vacuum that was starkly exposed during the 2023 parliamentary elections. The challenges faced by law enforcement agencies in addressing this high-profile deepfake incident have served as a powerful catalyst, highlighting the inadequacies of existing legal tools and accelerating the need to move towards specific, technologically-informed national regulation.

This incident revealed a fatal failure of reactive tools - a legal vacuum, the inability of law enforcement bodies to act quickly, and the impossibility of intervention during the election moratorium. Reliance on ex post legal tools (e.g., protection of personality rights, Criminal Code, GDPR) proved insufficient to prevent ex ante damage to the electoral process.

Still, the CSPV SAS research provides at least some insights into alternative, proactive strategies. The SAS project explicitly addressed the comparison of the effectiveness of "debunking" and "prebunking" in the context of disinformation about the war in Ukraine.

- **Debunking** - Represents reactive refutation (e.g., fact-checking) of disinformation that is already circulating. Its effectiveness is often limited by cognitive biases (e.g. continued influence effect).
- **Prebunking** - Is a proactive strategy based on the "cognitive inoculation theory". Its goal is to "inoculate" the population by exposing them in advance to a weakened form of a disinformation technique (e.g., showing them how deepfake or false context works), thereby building cognitive resistance before they are exposed to a real disinformation attack.

The failure in the 2023 deepfake incident and SAS psychological research together suggest that the state's strategy cannot rely solely on repression (which runs up against the speed of AI and jurisdictional barriers). It must necessarily be supplemented by prevention based on building cognitive resilience (prebunking). This shifts the focus of responsibility from law enforcement bodies also to bodies responsible for media literacy and strategic communication.

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)?

No. Slovak law does not yet explicitly define or recognize "deep fakes" or AI-generated media.[31] It relies on EU-level frameworks—the Digital Services Act (DSA) and Artificial Intelligence Act (AI Act)—for regulation of synthetic content. Specifically, the definition provided in Article 3, point 60 of the AI Act will become the operative legal standard in Slovakia. This article defines a deepfake as "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places or other entities or events and would falsely appear to a person to be authentic or truthful". This mechanism of legal harmonization is a key feature of EU regulation, allowing for a standardized definition across all member states without necessitating a separate, and potentially lengthy, parliamentary process in Slovakia to define the term itself.[32] Additionally, nevertheless, in an ongoing process of re-codification of private law, personality rights protection is also pondered upon with respect to the deep fake videos. However, the final outcome of the legislative process is still not at hand.

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

Not directly. Any accountability for misuse is pursued under existing laws—such as defamation, fraud, or criminal impersonation—not via specific statutes aimed at AI-generated content. Legal accountability is thus pursued under general statutes, which is an insufficient situation highlighted by the unsuccessful investigation into the 2023 election deepfake. So far, besides the criminal law tools, the misuse of such content can be addressed also through the data protection legislation. Especially, the General Data Protection Regulation (GDPR), or Regulation (EU) 2016/679,[33] serve as a possible, albeit indirect, tool for addressing the misuse of deepfakes. The creation and dissemination of a deepfake depicting an identifiable individual constitutes the processing of personal data. This triggers several key obligations under the GDPR. For instance, platforms hosting such content are likely required under Article 35 to conduct a data protection impact assessment due to the "high risk" posed by new technologies. Furthermore, they must implement "data protection by design and by default" as mandated by Article 25. Crucially, an individual depicted in a deepfake can invoke their Article 17 right to erasure (the "right to be forgotten") and demand its removal. A platform's failure to comply with a valid takedown request could expose it

[31] Turisová, Tatiana (2023): Deepfake technológia je už aj v slovenskom mediálnom prostredí, zákon ju zatiaľ nespomína. *Euractiv*. (online). (cited 2025-09-05). Available at: https://euractiv.sk/section/digitalizacia/news/deepfake-technologia-je-uz-aj-v-slovenskom-medialnom-prostredi-zakon-ju-zatial-nespomina/

[32] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEArelevance). (online). (cited 2025-09-05). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

[33] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance). (online). (cited 2025-09-05). Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

to significant administrative fines under the GDPR, creating a powerful legal and financial incentive for content removal that operates independently of any specific national "deepfake" law.[34]

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?

The most relevant legislation includes defamation under the Civil Code or Criminal Code. Still, there is no specific "deep fake" offence yet. Besides the courts and criminal law enforcement authorities, there are also other bodies involved in the fight against the misuse of deep fakes. For example, the National Bank of Slovakia has issued public warnings[35] about the increasing use of deepfake videos and voice clones in sophisticated investment scams, where fabricated endorsements from public figures are used to defraud investors. Such acts would be prosecuted as Fraud under § 221 of the Criminal Code. Similarly, while Slovakia has no specific law against adult deepfake pornography, the creation of such content using the identity of a minor would fall under existing sections of the Criminal Code, criminalizing the production and distribution of child pornography.

In civil law, the protection of personality under § 11 of the Civil Code offers a robust avenue for victims. A key advantage of this provision is that liability is objective; the victim is not required to prove the perpetrator's malicious intent. They only need to demonstrate that an unauthorized interference with their personality rights occurred and that this interference was capable of causing harm. Available remedies include a court-ordered cessation of the act, removal of the content, and satisfaction in the form of an apology or financial compensation for non-pecuniary damages.

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

The most prominent case is the criminal complaint filed by politician Michal Šimečka and journalist Monika Tódová following the 2023 election deepfake.[36] The police investigation, however, has been emblematic of the challenges faced by law enforcement. After an initial, widely criticized dismissal of the case, a supervising prosecutor ordered the investigation to be reopened. In late 2024, Denník N (the newspaper where Tódová works) reported that the police investigator had again proposed to halt the criminal proceedings, this time citing the inability to identify the perpetrator. The final decision now rests with the prosecutor.[37] This outcome underscores the significant technical and

[34] Mesarčík, Matúš – Zimen, Ondrej: Deep fake a ochrana súkromia. In: Acta Facultatis Iuridicae Universitatis Comenianae Tomus XXVII2/2019, p. 227-242. Available at: https://afi.flaw.uniba.sk/index.php/AFI/article/view/663/496

[35] Upozornenie: Čoraz častejšie „deepfake" videá testujú našu obozretnosť. *Národná banka Slovenska*. (online). (cited 2025-09-05). Available at: https://nbs.sk/aktuality/upozornenie-coraz-castejsie-deepfake-videa-testuju-nasu-obozretnost/

[36] Meaker, Morgan (2023): Slovakia's Election Deepfakes Show AI Is a Danger to Democracy. *Wired*. (online). (cited 2025-09-05). Available at: https://www.wired.com/story/slovakias-election-deepfakes-show-ai-is-a-danger-to-democracy/

[37] Kováčik, Timotej – Frankovská, Veronika (2024): How AI-generated content influenced parliamentary elections in Slovakia: The Slovak Police will investigate the recording for a third time. *Cedmo*. (online). (cited 2025-09-05). Available at: https://cedmohub.eu/how-ai-generated-content-influenced-parliamentary-elections-in-slovakia-the-slovak-police-will-investigate-the-recording-for-a-third-time/

jurisdictional hurdles in tracing the origins of anonymized, digitally manipulated content, effectively leaving the victims without criminal redress despite the clear harm caused.[38]

2.3 Preventive Measures and Oversight

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

There are not such requirements under Slovak national law. However, the EU AI Act (from August 2024) mandates that AI-generated or manipulated content must carry clear disclosure and, eventually, watermarking. The specific provision governing this requirement is Article 50 of the EU AI Act. It will mandate that users interacting with a deepfake are clearly informed that the content is artificially generated or manipulated. The regulation provides a nuanced approach, including exceptions for content that is part of an "overtly artistic, creative, satirical, [or] fictional" work. In such cases, the disclosure is limited to revealing the existence of manipulated content in a manner that does not impede its display or enjoyment, balancing transparency with artistic freedom.[39] Still, there is no actual case law or good practice examples available yet in Slovakia.

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

In July 2024, Slovakia cooperated with Meta to create a hybrid-threats center that alerts the company in case of AI-based disinformation campaigns.[40] Beyond the government's collaboration with Meta, the Slovak civil society and expert community have been proactive as well. In June 2025, the Association for Artificial Intelligence (ASAI), a non-governmental body, introduced Slovakia's first comprehensive ethical framework for AI. Developed in consultation with experts from academia, law, and media, this code is based on principles from international organizations like UNESCO and the Council of Europe. It establishes foundational rules for the responsible use of AI, with a strong emphasis on transparency, the clear labeling of AI-generated content, and the protection of personal data. While voluntary, this code represents a significant step in establishing industry standards for ethical AI development and deployment in Slovakia.[41]

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

Platforms operating in Slovakia must comply with the EU DSA and AI Act rules, which include transparency obligations and robust moderation standards. Slovak platforms participate voluntarily in EU-led trust frameworks. Platforms are foremost subject to the EU-wide Code of Practice on Disinformation, which was strengthened in 2022 and includes commitments related to emerging threats like AI-driven manipulation. Furthermore, the 2024 Annual Report of the Council for Media Services (RPMS), in its new capacity as the Slovak Digital Services Coordinator, highlights that a key part of its mandate will be to oversee the systemic risk assessments conducted by Very

[38] Łabuz, Mateusz – Nehring, Christopher (2024): On the way to deep fake democracy? Deep fakes in election campaigns in 2023. *Eur Polit Sci* 23, 454–473 (2024). (online). (cited 2025-09-05). Available at: https://link.springer.com/article/10.1057/s41304-024-00482-9

[39] Waszak, Marcin (2024): Millions in fines for failing to comply with AI Act – Check out the new regulations!. *Dudkowiak&Putyra*. (online). (cited 2025-09-05). Available at: https://www.dudkowiak.com/blog/millions-in-fines-for-failing-to-comply-with-ai-act-check-out-the-new-regulations/

[40] Slovakia partners with Meta to combat fake videos with Pellegrini and Čaputová. *The Slovak spectator*. (online). (cited 2025-09-05). Available at: https://spectator.sme.sk/politics-and-society/c/slovakia-partners-with-meta-to-combat-fake-videos-with-pellegrini-and-caputova

[41] ASAI. (online). (cited 2025-09-05). Available at: https://www.asai.sk/en/

Large Online Platforms (VLOPs) under the DSA. These assessments must explicitly address the risks posed by AI in amplifying disinformation, making the management of AI-generated content a de facto regulatory priority for the RPMS.[42]

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?

As already mentioned, two days before the September 2023 election, AI-generated audio falsely attributed a vote-rigging plot to Michal Šimečka and journalist Monika Tódová. This occurred during a campaign moratorium, severely limiting its timely debunking. While the direct impact of the deepfake on the election's outcome is difficult to quantify and may be overstated, its effect on the political and media discourse was profound. The incident's impact was significantly magnified by its amplification through a hybrid media ecosystem. The audio was shared on a Telegram account associated with presidential candidate Štefan Harabin and was further disseminated by other politicians on platforms like Facebook. This demonstrates how political actors can serve as key nodes in legitimizing and spreading AI-generated disinformation, transforming a piece of synthetic media into an important political tool.

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

There are no explicit domestic rules for AI-influenced electoral campaigns. General regulations on fair advertising, defamation, and election silence (48-hour moratorium) apply – but no specific transparency or disclaimer rules for AI content were introduced yet.

A potential, though legally uncertain, avenue for prosecution in case of future abuse of AI-generated content in electoral campaign could be the criminal offense of Obstruction of the Preparation and Conduct of Elections (§ 345 of the Criminal Code). This offense could theoretically apply if it can be proven that a deepfake was used with "deceit" to prevent voters from exercising their right to vote. However, legal experts highlight a significant obstacle: the term "deceit" is not statutorily defined and is generally interpreted as an intentional act of inducing an error in another person. There is no established judicial precedent in Slovakia applying this concept to cases of large-scale disinformation aimed at influencing entire elections, making its application in the context of a deepfake legally untested and challenging.

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?

Slovakia is currently drafting a national AI Act to implement the EU AI Act, designating supervisory authorities (Personal Data Protection Office, Public Defender of Rights) and embedding AI content transparency and watermark requirements. The country plans to modernize its personal data law and establish ethical guidelines, including a governmental working group to combat disinformation

[42] 2024 Výročná správa o činnosti Rady pre mediálne služby podľa článku 55 DSA za rok 2024. *Rada pre mediálne služby*. (online). (cited 2025-09-05). Available at: https://rpms.sk/sites/default/files/2025-04/VS_o_cinnosti_RpMS_podla_clanku_55_DSA_0.pdf

using AI tools.[43] No domestic bill specifically criminalizes deep fakes yet, but EU frameworks are surely catalyzing national implementation efforts.

The legislative process for this national implementation law is run under the number LP/2025/401[44] and is currently in the inter-ministerial comments phase. The draft law designates the Ministry of Investments, Regional Development, and Informatization (MIRRI) as the central supervisory authority and single point of contact for AI regulation. It also establishes sectoral supervisory roles for other bodies, including the National Security Authority (NBÚ) and the Data Protection Office. Key provisions include the creation of a regulatory sandbox for AI and the introduction of new obligations for operators of high-risk AI systems, such as requirements for monitoring and transparency when used by public authorities. The law is proposed to take effect from 1 January 2026, signaling a clear timeline for Slovakia's transition to a more structured and proactive AI regulatory environment.

[43] Slovakia. *Bird&Bird*. (online). (cited 2025-09-05). Available at: https://www.twobirds.com/en/capabilities/artificial-intelligence/ai-legal-services/ai-regulatory-horizon-tracker/slovakia

[44] PI/2025/2 Návrh zákona, ktorým sa upravujú inštitucionálne podmienky, pôsobnosť orgánov, práva a povinnosti subjektov v súvislosti s využívaním systémov umelej inteligencie. (online). (cited 2025-09-05). Available at: https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/PI/2025/2; LP/2025/401 Návrh zákona o organizácii štátnej správy v oblasti umelej inteligencie a o zmene a doplnení niektorých zákonov. (online). (cited 2025-09-05). Available at: https://www.slov-lex.sk/elegislativa/legislativne-procesy/SK/LP/2025/401

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

The Slovak legal framework is built upon a strong constitutional prohibition of censorship, a principle that has been consistently upheld and narrowly interpreted by the nation's highest courts. However, this foundational safeguard is facing a significant test from recent legislative initiatives aimed at restructuring public media and regulating civil society. This has created a palpable tension between the state's asserted need to regulate the information space and the constitutional and international standards protecting freedom of expression, setting the stage for potentially landmark constitutional confrontations.

There was identified also another key tension in the Slovak legal order - the conflict between the constitutional prohibition of censorship (Article 26 of the Constitution of the Slovak Republic) and (2) controversial state interventions (such as the STVR Television and Radio Act or other legislative proposals of the coalition party SNS), which are perceived by civil society and the opposition as an attack on freedom of expression.[45]

However, new empirical data (CEDMO) reveals that this two-dimensional conflict is actually a more complex "trilemma" by adding a third actor - public opinion. The CEDMO Trends survey (November 2024) found that 74% of the Slovak population agrees that the state should restrict media outlets that spread disinformation. Thus, almost three-quarters of the public actively desire a type of regulation that legal experts and constitutional courts often interpret as inadmissible censorship or a restriction contrary to the principles of freedom of expression. The government can therefore politically legitimize its controversial regulatory steps as fulfilling the majority will of the people. This creates a dangerous situation where the protection of constitutional principles of freedom of expression (Art. 26) comes into direct conflict not only with the executive power but also with the attitude of a significant majority of the public.

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)?

Article 26 paragraph 3 of the Constitution of the Slovak Republic explicitly states: "Censorship is prohibited." This forms the primary constitutional safeguard against prior restraint by the state. However, paragraph 4 of the same article allows for exceptions for reasons such as protection of national security, public order, morals, and the rights and freedoms of others. These exceptions must be in line with the principles of a democratic society. The scope of these permissible exceptions has been strictly defined by the judiciary. In the landmark decision **PL. ÚS 7/96**, the Constitutional Court of the Slovak Republic established that any limitation on freedom of expression must be interpreted narrowly and must satisfy a rigorous proportionality test.[46] This precedent is the cornerstone of Slovak jurisprudence on this issue, creating a high constitutional

[45] (cited 2025-09-05). Available at: https -//cedmohub.eu/cedmo-trends-slovakia-the-14th-wave-as-seen-by-ipsos/

[46] Decision of the Constitutional Court of the Slovak Republic, file no. II. ÚS 7/96. (online). (cited 2025-09-05). Available at: https://merit.slv.cz/PL.%C3%9AS7/96

threshold that any legislative or administrative restriction on speech must overcome. It requires authorities to demonstrate not only that a restriction serves a legitimate aim but also that it is the least intrusive means necessary to achieve that aim.

3.2 Judicial Interpretations and Key Cases

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

Slovak legal discourse on freedom of expression is characterized by persistent uncertainty regarding the precise interpretation of the term "censorship." This uncertainty, which stems in part from the lack of a legal definition of censorship in the legal system, has led to what can be described as "dual jurisprudence" of the Constitutional Court of the Slovak Republic. The core of the dispute lies in the relationship between Article 26(3) of the Constitution of the Slovak Republic ("Censorship is prohibited") and Article 26(4), which allows for lawful restrictions on freedom of expression for reasons such as the protection of public order or state security. This dispute is most evident when comparing two different approaches in decisions from 2009 and 2019.

The first, and now older, line of interpretation is represented by the ruling of the Constitutional Court Senate, ref. no. III. ÚS 42/09 of June 2, 2009. Although this was an ex-post (subsequent) intervention and not typical preventive censorship, the Constitutional Court directly linked this procedure to the prohibition of censorship. According to the analysis of this decision, the court stated that the consequence of the procedure of a state authority assessing the "correctness" or accessibility of expressed opinions is the "introduction of a new form of censorship." According to analyses of this decision, the court found that the consequence of the procedure of a state authority assessing the "correctness" or accessibility of expressed opinions is the "introduction of censorship," which is explicitly excluded under Article 26(3). With this ruling, the court applied the term "censorship" broadly, including subsequent interventions by public authorities, thereby supporting an extensive interpretation of the constitutional prohibition. This line of reasoning admits that even subsequent, politically motivated state intervention in the content of expression can be classified as unconstitutional censorship.

The second, more modern and currently dominant line of interpretation is represented by the plenary ruling of the Constitutional Court, ref. no. PL. ÚS 26/2019 of May 26, 2021. The facts of the case were ideal for testing censorship, as it involved a clear preventive (ex-ante) prohibition on the dissemination of information imposed by law. Nevertheless, the plenary session of the Constitutional Court chose a diametrically different methodological approach than the Senate in 2009. The Court did not address the question of whether this moratorium constituted "censorship" within the meaning of Article 26(3). Instead, it proceeded directly to the proportionality test under Article 26(4). It therefore assessed the moratorium exclusively as a "lawful restriction" on freedom of expression and examined whether it pursued a legitimate aim and whether it was "necessary in a democratic society."

This plenary ruling de facto confirmed the strict, so-called orthodox model of interpretation (dominant in the Czech Republic), which perceives Paragraph 3 (prohibition of censorship) and Paragraph 4 (lawful restrictions) as two separate categories. According to this approach, "censorship" (Paragraph 3) is absolutely prohibited, but it is understood narrowly as an institutional, preventive system of content approval by the state. Conversely, all other interventions, whether subsequent (sanctions) or preventive (such as a moratorium), are considered only as "restrictions" under Paragraph 4, and their only test of constitutionality is the test of proportionality. With this decision, modern Slovak case law has leaned toward the view that

preventive state intervention (such as a moratorium) is not called censorship, but a legal restriction that must pass the test of necessity.

Slovak courts have generally respected the constitutional ban on censorship but have allowed content restrictions when justified. Domestic courts apply a proportionality test in such cases. The *Ringier Axel Springer* cases (e.g., applications **no. 41262/05**, **37986/09**, and **26826/16**)[47] have been pivotal. In these rulings, the ECtHR repeatedly found that Slovak courts had violated Article 10 of the European Convention on Human Rights (ECHR) by failing to properly balance the right to privacy with the public's interest in receiving information on matters of public concern. These judgments compelled the domestic judiciary to adopt a more nuanced approach, distinguishing between factual statements and value judgments and affording greater protection to speech on matters of public interest.

Domestically, the Constitutional Court established foundational principles in its decision **II. ÚS 28/96**, which defined freedom of expression as a fundamental *political* right, essential for the formation of public opinion and the proper functioning of a democratic society. This classification as a political right underscores its elevated status and the high degree of protection it receives under the Slovak constitutional order.[48]

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

For example, in the Milan Mazurek case (2019), the Supreme Court upheld a hate speech conviction, arguing that freedom of expression does not protect speech inciting hatred or discrimination. In its judgment, the Supreme Court upheld the conviction of Milan Mazurek for making xenophobic and defamatory statements against the Roma minority, qualifying them as the criminal offense of defaming a nation, race, and belief. The court's reasoning explicitly stated that freedom of expression is not an absolute right and does not provide a shield for hate speech that incites discrimination and violence. This judgment authoritatively established that the criminal prosecution of such speech is not unconstitutional censorship but a necessary and legitimate limitation on expression, justified for the protection of the rights of others and the maintenance of public order.[49]

3.3 Scope and Enforcement

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

Several bodies play a role in the enforcement of laws related to speech and content. The Constitutional Court of the Slovak Republic is the ultimate guardian against unconstitutional censorship. Ordinary general courts have the power to order the removal of unlawful content, such as defamation or hate speech, following civil or criminal proceedings. The Council for Media Services (RPMS) is the administrative body responsible for regulating audiovisual media and online platforms and can issue administrative sanctions for violations of media law.

---

[47] Decision of the ECHR, file no. 41262/05. (online). (cited 2025-09-05). Available at: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-105825%22]}

[48] ÚS SR Nález Ústavného súdu Slovenskej republiky, sp.zn. II. ÚS 28/96 z 12. mája 1997. (online). (cited 2025-09-05). Available at:https://www.slov-lex.sk/sudne-rozhodnutia/judikaty/69f1db73-8d19-4c96-b7f0-74b41f43a3f9

[49] Mikušoviš, Dušan (2019): Mazurek v parlamente končí, súd mu potvrdil vinu za rasistické reči v rádiu. *Dennikn*. (online). (cited 2025-09-05). Available at: https://dennikn.sk/1571676/mazurek-v-parlamente-konci-sud-mu-potvrdil-vinu-za-rasisticke-reci-v-radiu/

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

These bodies apply a case-by-case analysis based on the principle of proportionality. Content removal is only deemed permissible if it is based on a specific legal provision and is the result of a court order or a reviewable administrative decision. In cases involving a conflict between fundamental rights, such as freedom of expression versus the protection of personality, the Constitutional Court requires a "just balance" to be struck (see decision PL. ÚS 7/96).

The Supreme Administrative Court, when reviewing sanctions (also imposed by the RPMS), exercises "full jurisdiction," meaning it is not bound by the regulator's factual findings and can conduct its own assessment of the evidence, including reviewing the broadcast content itself (see e.g. judgment 5Sžo/39/2016).

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

All content removals must be legally grounded and subject to judicial review. Administrative bodies like RPMS must follow due process. Content creators may appeal or contest restrictions. Any administrative decision to restrict content, whether by the RPMS or the NBÚ, can be challenged in the administrative courts. Furthermore, the DSA, as implemented in Slovakia, provides users with multiple avenues of redress against platform decisions, including internal appeals, out-of-court dispute settlement, and the right to file a complaint with the RPMS or a court.[50]

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?

Yes, there was at least one case. During the 2023 parliamentary elections, a deepfake audio targeting opposition leader Michal Šimečka could not be removed quickly due to the 48-hour pre-election silence. Legal uncertainty delayed intervention. The combination of legal uncertainty, the novelty of the threat, and the lack of a rapid response mechanism created a situation where authorities were unable to act decisively to curb the spread of the harmful disinformation before polls opened, illustrating a practical challenge where legal frameworks designed to protect speech inadvertently hindered a response to a direct attack on the democratic process.

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

Yes, two recent legislative initiatives have raised significant concerns about state overreach and de facto censorship.

1. The 2024 law dissolving the public broadcaster RTVS and creating a new entity, Slovenská televízia a rozhlas (STVR), has been widely condemned by international press freedom organizations. The European Broadcasting Union (EBU) and the International Press Institute (IPI) described it as a "thinly veiled attempt to turn the Slovak public service broadcaster into state-controlled media". The law, which allows the government to replace the broadcaster's leadership through a new council with government-nominated

[50] Slovakia: Law No. 264/2022 on Media Services including content moderation regulation enters into force. *Digital Policy Alert*. (online). (cited 2025-09-05). Available at: https://digitalpolicyalert.org/event/28951-law-no-2642022-on-media-services-including-content-moderation-regulation-enters-into-force

members, is currently under review by the Constitutional Court, signifying a serious constitutional challenge to the measure.

2. A bill introduced by the SNS party in 2024 would require non-governmental organizations (NGOs) receiving over €5,000 annually from foreign sources to be labeled as "organizations with foreign support". Civil society organizations like VIA IURIS have analyzed the proposal and concluded it is discriminatory and likely unconstitutional, drawing parallels to repressive laws in Russia and Hungary designed to stigmatize and silence critical voices.[51] In the end, a milder version was adopted, forcing the NGOs to report the sourced of their funding.

3.5 Future Outlook

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

Yes – the 2023 deepfake audio case sparked significant domestic debate in Slovakia regarding whether existing laws are fit for the AI era. Commentators, journalists, and NGOs in Slovakia have highlighted the need to adapt censorship and free-expression rules to handle digital disinformation more effectively – without undermining constitutional protections. E.g., Pavol Szalai argued that Slovakia is "a laboratory of political deep fakes… the way out is stronger regulation of digital platforms and AI, which make 'alternative' information impactful.[52] The Harvard Misinformation Review, in its "Beyond the Deepfake Hype" article, labels the Slovak case a "test case" of democratic vulnerability, urging policymakers to rethink how laws differentiate between harmful and merely offensive digital content.[53]

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

AI-powered content moderation tools - The 2023 election deepfakes revealed critical gaps: human fact-checkers lacked tools to rapidly detect AI-manipulated audio, while platforms like Meta found only 50% of flagged hate speech was taken down before the vote. This has driven calls for more automated detection and response systems.

The proliferation of generative AI tools for creating sophisticated synthetic media is forcing a re-evaluation of what constitutes "evidence" and how to maintain a trusted information ecosystem. This is driving calls for **mandatory labeling and watermarking of AI-generated content, as envisioned by the EU AI Act.** The sheer volume and speed of online content make manual moderation untenable. This is increasing the reliance on AI-driven content moderation systems. However, this raises new censorship concerns related to algorithmic bias, lack of transparency, and

[51] Slovak politicians introduce law on labelling of NGOs with foreign funding (Zeitgeist 2.). *VIA IURIS*. (online). (cited 2025-09-05). Available at: https://viaiuris.sk/aktuality/zeitgeist-newsletter/slovak-politicians-introduce-law-on-labelling-of-ngos-with-foreign-funding-zeitgeist-2/

[52] Rojo, Magdalena (2024): Inside Slovakia's crackdown on free media. *Fairplanet*. (online). (cited 2025-09-05). Available at: https://www.fairplanet.org/story/inside-slovakias-crackdown-on-free-media-fico-assassination-attempt/

[53] De Nadal, Lluis – Jančárik, Peter (2024): Beyond the deepfake hype: AI, democracy, and "the Slovak case". *Misinformation review*. (online). (cited 2025-09-05). Available at: https://misinforeview.hks.harvard.edu/article/beyond-the-deepfake-hype-ai-democracy-and-the-slovak-case/

the potential for automated systems to erroneously remove legitimate speech, necessitating robust human oversight and appeal mechanisms as mandated by the DSA.

4
NATIONAL REGULATION OF INTERNET CONTENT

Slovakia's national framework for regulating internet content, particularly through website blocking, presents a compelling case of an "implementation gap." While the country has developed a legal structure to block harmful content, this framework is significantly undermined in practice. A documented lack of institutional capacity and a systemic lack of transparency have resulted in a system that has seen limited and opaque application, raising questions about both its effectiveness and its accountability.

The primary tool of national regulation is the power of the National Security Authority (NBÚ) to block websites (domains). However, besides limiting this competence first by time (it was allowed only until September 2022) and then by the need for a proposal by a competent law enforcement body, new data additionally shows that this approach is outdated because the main content battle has shifted from the open web to the closed ecosystems of multinational platforms.

The first extensive European study SIMODS (Structural Indicators to Monitor Online Disinformation Scientifically), in which the Slovak fact-checking project Demagog.sk participated, brought alarming findings in 2025:

- **Dominance of platforms** - The highest prevalence of disinformation on topics of public interest was recorded on the TikTok platform (20% of posts). Other platforms like X (Twitter), Facebook, Instagram, and YouTube were around 10%, while LinkedIn was only at 2%.
- **Slovakia as a negative anomaly** - Compared to other countries in the study consortium, disinformation on the TikTok and Facebook platforms occurred significantly more often in Slovakia.
- **Algorithmic reward** - A key finding is that accounts spreading disinformation achieved (with the exception of LinkedIn) greater reach and more interactions than credible sources. Disinformation content is thus algorithmically rewarded by existing systems.

Table 2 - Comparison of Disinformation Prevalence on Online Platforms (2025)

Platform	Share of Disinformation (on topics of public interest)
TikTok	20 %
X (Twitter)	~10 % (32 % including borderline content)
Instagram	~10 %
YouTube	~10 %
Facebook	~10 % (Note - significantly more frequent in SR)
LinkedIn	2 %

Source - SIMODS Study, 2025

This data in combination with the deepfake incident (primarily disseminated via Telegram and Facebook) proves that national regulation focused on domain blocking is insufficient. Modern disinformation is atomized and spreads in closed, algorithmically managed ecosystems that are beyond the reach of this tool. Effective regulation must therefore shift from national domain blocking to transnational algorithmic regulation, i.e., to the rigorous enforcement of the Digital Services Act (DSA).

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 legal instrument is the Cyber Security Act (Act No. 69/2018 Coll.), which allows the National Security Authority (NBÚ) to block websites containing "harmful content" or representing cybersecurity threats, based on a motion from competent law enforcement bodies. The regulation of social media and other online platforms is now principally governed by the Media Services Act (No. 264/2022) which implements the EU's Digital Services Act (DSA).

Additionally, specific legislation allows for the blocking of websites offering illegal online gambling. The Gambling Regulatory Authority (GRA) is authorized to supervise the provision of prohibited offers and compliance with the obligations of Act No. 30/2019 Coll. on gambling and on amendments and supplements to certain acts and special regulations (Act No. 492/2009 Coll. on payment services, as amended, and Act No. 452/2021 Coll. on electronic communications, as amended), which are related to the provision of prohibited offers and which apply to supervised entities – providers of electronic communications networks and services and providers of payment services. The Authority publishes the list of prohibited websites and the list of prohibited numbers on its website on the first working day of the week according to the status as of the last day of the previous week.[54] Under § 86 of the Act on gambling, the GRA shall not include in the list of prohibited websites a supervised entity that proves that it does not provide a prohibited offer or proves that it has terminated the provision of a prohibited offer. When exercising supervision over the provision of prohibited offers, the GRA is entitled to request documents for the exercise of supervision from the payment service provider, namely the identification of the payment service user and other information about the payment service user who is the supervised entity. A person providing electronic communications networks and electronic communications services (basically an internet service provider) shall be obliged, on the basis of a court order issued at the request of the GRA, to prevent access to a website through which a prohibited offer is provided. The payment service provider shall be obliged, on the basis of a court order issued at the request of the Office, to prevent the execution of a payment transaction or other payment service in favour of an account used by the person providing the prohibited offer for the purpose of accepting a deposit when providing the prohibited offer and in relation to a merchant, if payment transactions are carried out through a merchant for the purpose of accepting a deposit when providing the prohibited offer. The actual mechanism of blocking under this Act additionally requires a judge to issue an order to the internet service providers to block, whereby no appeal shall be allowed against a court order.

Finally, under § 34 of the Act no. 108/2024 Coll. on consumer protection, if, as a result of a breach of the obligation of the supervised person, the collective interests of consumers are harmed or if there is a risk of serious harm to the collective interests of consumers, the supervisory authority is entitled to request in writing the supervised person who operates or on whose behalf the online

[54] List of blocked websites. (online). (cited 2025-09-05). Available at: https://www.urhh.sk/urad/dozor-a-kontrola/zakazane-ponuky/zoznam-blokovanych-webov/

interface is operated to remove or change the content published on the online interface, to limit or prevent consumers' access to the online interface, to access some or all of the functions or services of the online interface, or to publish a warning for consumers accessing the online interface, within a period specified by the supervisory authority. The supervisory authority shall publish the notice referred to in the first sentence on its website within three days if it has not been able to identify the supervised person who operates the online interface or on whose behalf the online interface is operated; the last day of the period shall be deemed to be the day of receipt of the notice. If the purpose cannot be achieved otherwise and the supervised person does not comply with the request or if it is obvious from all circumstances that the procedure will not result in immediate remedial action, or upon request or in a coordinated procedure pursuant to a special regulation, the supervisory authority may issue a measure to block. The supervised person may submit a written objection to the supervisory authority that issued the blocking measure within five working days of the date of delivery of the blocking measure if he or she disagrees with the blocking measure. The objection must be substantiated in substance. The supervised person may extend, amend or supplement the scope of the objection to which he or she is challenging the blocking measure and the grounds for the objection only until the expiry of the period set for submitting the objection. An objection submitted in good time does have a suspensive effect. The supervisory authority decides on the objection pursuant to paragraph 6 within five working days of the date of its delivery. The supervisory authority's decision on the objection is final and not subject to appeal.[55]

This creates a poly-authority structure, with the NBÚ handling security-related blocking and the Council for Media Services (RPMS) overseeing platform compliance under the DSA. Additionally, specific legislation permits the domain-level blocking of websites offering illegal online gambling by the GRA.[56] Finally, the bodies of consumer protection can decide on blocking of websites where this leads to a harm to consumers.

4.2 Scope of Website Blocking

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

NBÚ can block websites in cases of cybersecurity threats, hybrid disinformation campaigns, illegal unlicensed gambling, or for the sake of protection of consumers – however, in all these instances it can only do so upon request from a competent authority. Under the Cyber Security Act, the NBÚ was originally allowed initiate blocking if a website is found to be disseminating "harmful content" or engaging in "harmful activity." This was defined broadly to include not only technical cyber threats but also activities that constitute a "hybrid threat" and could harm the security, foreign policy, or economic interests of the Slovak Republic. This explicitly includes the dissemination of "serious disinformation". However, this competence was in use only from the start of the war in Ukraine until September 2022. Since then, only blocking upon a motion from a competent law enforcement body is possible.

[55] Currently, the Slovak Business Inspection publishes only a List of risky internet commerce websites. (online). (cited 2025-09-05). Available at: https://www.soi.sk/sk/informacie-pre-verejnost/internetove-obchody/rizikove-internetove-obchody.soi

[56] Sokol, Pavol – Bachňáková Rózenfeldová, Laura (2025): Content blocking mechanism in cybersecurity: Slovakia case study. *SpringerOpen*. (online). (cited 2025-09-05). Available at: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-025-00190-x

Several provisions in the Cybersecurity Act thereby refer to the so-called Blocking Rules, which have not yet been published in legal form.[57] The legal regulation nevertheless contains a relatively precise identification of the requirements for a blocking decision and the requirement of purposefulness, proportionality, and effectiveness.

As already mentioned, the NSA could have, on its own initiative, decide on blocking only with effect until September 30, 2022. This limit does not apply to blocking upon the initiative of another authority, though. It is interesting to note that in the case of blocking at the request of another entity: "the costs associated with the blocking based on the applicant's request and the liability for damage caused by the blocking shall be borne by the applicant." This is a relatively unique transfer of responsibility in the exercise of state power in the Slovak legal system to the reporting entity.

At the same time, it should be noted that even after the major amendment to the Cyber Security Act due to the necessity of transposing the NIS 2 Directive, this legal provision remained unaffected and is still part of the Slovak legal system.

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?

Yes, the definitions of "harmful content" and "hybrid threat" in the Cyber Security Act are notably broad and lack precise, objective criteria. This breadth has been a point of criticism from legal experts and civil society organizations, who argued it creates a risk of arbitrary application. Probably that is also the reason why no website is currently being blocked by the NBÚ. The other authorities, like the GRA or the Business Inspection have their own blocking mechanisms and can enforce blocking even without the need for the NBÚ.

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.

Blocking is currently an administrative action to be performed by NBÚ (or GRA or relevant consumer protection bodies). Based on Act No. 69/2018 Coll. on Cybersecurity, the NBÚ can block a website, however, the legal framework has evolved to make this process less "ad hoc" and more structured, especially regarding the need for motion by another body for the blocking.[58]

The above-mentioned shortcomings of competences of NBÚ were to be eliminated by a proposed amendment, through which the state sought to introduce a systemic measure for blocking harmful content. The proposed legal regulation no longer contained the term serious disinformation, but one could classify this phenomenon as hybrid threats with a certain intensity. The positive thing was that, according to the proposed amendment, blocking required the consent of the Court and the National Security Service was to publish all decisions on its website. However, in the end, the draft amendment in question was never enacted.[59]

[57] Being published only on the website of the NBÚ. (cited 2025-09-05). Available at: https://www.nbu.gov.sk/data/att/1135.pdf

[58] Act. No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts. (online). (cited 2025-09-05). Available at: https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2018/69/

[59] Draft Act amending and supplementing Act No. 69/2018 Coll. on Cybersecurity and on Amendments to Certain Acts, as amended – new wording. *Úrad vlády Slovenskej republiky*. (online). (cited 2025-09-05). Available at: https://rokovania.gov.sk/RVL/Material/27764/1

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

The ability to order website blocking by the tools of NBÚ have law the already mentioned enforcement bodies under special laws (gambling, consumer protection). NBU is not using this competence currently. Concerning both gambling and consumer protection, the implementation of the blocking order is first in the hands of the website operators, but in the second place, if the operators do not comply, blocking is also the mandatory responsibility of all internet service providers (ISPs) operating in Slovakia. They can be requested to block the websites by the respective gambling and consumer protection authorities.

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

NBÚ, like many specialized government agencies, faced challenges in terms of sufficient human resources and technical expertise for such a demanding and rapidly evolving agenda as cybersecurity and content moderation. The sheer volume and speed of online content, especially disinformation, require continuous monitoring, analysis, and rapid response capabilities. Agencies like NBÚ are continuously trying to build capacity, invest in technology, and train staff. However, whether they are "well-staffed" is a subjective assessment, and it's likely they always face pressure to do more with potentially limited resources given the scale of the threat.

The 2024 Annual Report on Cybersecurity in the Slovak Republic in this respect highlighted some systemic issues in public administration, including a lack of comprehensive risk management and insufficient resources.[60] An academic analysis in the EURASIP Journal on Information Security directly attributes the limited practical application of the blocking mechanism to insufficient technical and human resources within the NBÚ. These findings indicate that while the legal authority exists, the institutional capacity to effectively wield it is constrained.

Hence, the only body that actually performs blocking of websites is the GRA, which blocks the illegal gambling and betting websites.

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

This is a critical point of public debate and legal scrutiny. While the law outlines a process of blocking by the NBÚ, the transparency of criteria has been a subject of concern. The specific, detailed methodology or criteria used to assess "harmful content" or a "hybrid threat" are not public.[61] This lack of transparency has been criticized. In conclusion, while a legal process exists, the transparency of the specific criteria and the public availability of detailed reasons for each individual blocking decision have been areas where the current framework is criticized for not being sufficiently transparent.[62] Still, given the fact that NBÚ can currently block the websites only upon a motion form another authority, whereby these authorities mostly have their own routes and tools to block, the actual NBÚ competence to block is not being used in the moment.

Criteria for blocking in case of gambling or consumer protection are regulated by the respective acts of the parliament on gambling and on the consumer protection.

---

[60] Správa o kybernetickej bezpečnosti v Slovenskej republike v roku 2024. *Národný bezpečnostný úrad*. (online). (cited 2025-09-05). Available at: https://www.nbu.gov.sk/data/att/3305.pdf

[61] General rules are available at: https://www.nbu.gov.sk/data/att/1135.pdf (online). (cited 2025-09-05).

[62] LIBERTIES RULE OF LAW REPORT 2023 SLOVAKIA. *VIA IURIS*. (online). (cited 2025-09-05). Available at: https://dq4n3btxmr8c9.cloudfront.net/files/h4j5hd/RuleOfLaw_Report_2023_Slovakia_EU.pdf

4.3 Implementation and Enforcement

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

Blocking is conducted primarily through DNS-level filtering, with providers implementing IP or URL filtering upon NBÚ's order,[63] where ISPs are ordered to prevent the resolution of the targeted domain name. The blocking orders can also include specific IP addresses associated with the service. In the case of the Hlavné Správy block, the order also reportedly required the hosting provider to deny access to the site's administrative interface and to withhold backups and databases from the operator, representing a more comprehensive form of technical intervention. The operator of Hlavné správy thereby only challenged the lack of reasons before the administrative court, whereby the administrative court finally decided on this only after a number of years, confirming the actual lack of proper reasons for blocking. Still, the blocking was in force for a short period of time only, since the NBÚ itself lost the competence to block the websites by September 2022.

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

The entities concerned have the right to file an administrative lawsuit against the blocking decision, in the form of a general administrative court action. However, the action has in general no suspensive effect.

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?

NBÚ can act without issuing prior warnings or correction windows. The blocking decision is delivered directly to the internet service providers who are to implement it. The other authorities, mostly in the area of gambling and consumer protection, issue a warning to the concerned operators, and only once the warning does not lead to correction, they approach the internet service providers.

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

Legally, only whole domains may be blocked – not individual URLs or subpages. This means that access to the entire website is blocked.

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

Providers operating in Slovakia apply the block; for foreign hosts, NBÚ may use international cooperation channels (such as European court orders or mutual legal assistance mechanisms), though specifics are not public.

[63] Top privacy s.r.o. (2021): Amendment to the Cyber Security Act. *Top privacy*. (online). (cited 2025-09-05). Available at: https://www.legalfirm.sk/en/top-privacy/clanok/amendment-cyber-security-act

4.4 Transparency and Accountability

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

The list of blocked websites is to be published. As of now, no blocking takes place under the Cybersecurity Act, though.[64] The GRA publishes each week a list of blocked websites. The consumer protection authorities rather use official list of risky websites instead of actually blocking them.

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

Decisions may be challenged in administrative court, though such appeals do **not suspend** the block in general, which means that the block remains in effect until the court's decision.

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

No, there is no avenue to challenge blocking in other way than via administrative courts. The general rules of administrative procedure do not apply to blocking.

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

Under Sec. 27c(2) of the Cybersecurity Act, the blocking is set for a specific time limit, including the possibilities to lift up the blocking. Similarly the act on gambling and the act of consumer protection also rule that the blocking should only be temporary.

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

The Administrative Court can review blocks upon an administrative court action, no separate oversight body exists beyond this judicial channel.

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 — there are both academic studies and official analyses that assess the real-world impact and limitations of Slovakia's internet content regulation. A detailed case study published in the EURASIP Journal on Information Security (2025) analyzes Slovakia's blocking mechanism under the Cyber Security Act. The study notes that only a small number of blocking decisions (four) were issued in practice, measures included illegal gambling sites and pro-Russian disinformation platforms and despite legal powers, NBÚ demonstrated limited effectiveness due to lack of published decision details and insufficient technical and staffing capacity.[65]

[64] Zoznam blokovaných subjektov. *Národný bezpečnostný úrad*. (online). (cited 2025-09-05). Available at: https://www.nbu.gov.sk/zoznam-blokovanych-subjektov/

[65] Sokol, Pavol – Bachňáková Rózenfeldová, Laura (2025): Content blocking mechanism in cybersecurity: Slovakia case study. *SpringerOpen*. (online). (cited 2025-09-05). Available at: https://jis-eurasipjournals.springeropen.com/articles/10.1186/s13635-025-00190-x

The Freedom House Nations in Transit 2023 report criticizes the NBÚ's actions, stating that while they did block several disinformation outlets (e.g., Hlavné Správy), the non-disclosure of criteria and process sparked controversy and raised doubts regarding the practice's legitimacy.[66]

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

Site operators resorted to mirror domains, VPN usage, Telegram channels, reducing the block's impact.[67]

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

Domestic providers participated in consultation rounds, stressing technical constraints and the need for clearer norms.

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?

A NIS2-based amendment (effective as of Jan 1, 2025) further extended security obligations to thousands of other entities in 18 economic sectors. The aim was to strengthen the overall level of cybersecurity in the country. Website blocking was thereby not affected by the amendment and no new amendment is currently being drafted in this regard.

4.7 Practical and Ethical Considerations

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

Civil society organizations, digital rights experts, and commentators have repeatedly expressed concerns that broad and vaguely defined blocking powers could lead to so-called collateral censorship, whereby legitimate speech could be blocked alongside harmful content. They also point to the possible chilling effect, whereby authors and platforms could start avoiding sensitive topics for fear of possible blocking, which could lead to self-censorship and a restriction of legitimate public debate.

[66] Hlatky, Roman: Nations in Transit 2023, Slovakia. *Freedom House*. (online). (cited 2025-09-05). Available at:https://freedomhouse.org/country/slovakia/nations-transit/2023

[67] Cory, Nigel (2021): Website Blocking in Europe: Debated, Tested, Approved, and Defended. *ITIF*. (online). (cited 2025-09-05). Available at:https://itif.org/publications/2021/05/07/website-blocking-europe-debated-tested-approved-and-defended/

5
NATIONAL IMPLEMENTATION OF RELEVANT EU REGULATIONS CONCERNING INTERNET CONTENT

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?

Slovakia amended the Criminal Code and aligned the Cyber Security Act to implement the obligation for prompt takedown of terrorist content, incorporating the EU's one-hour removal rule.[68]

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

The Media Services Act (No. 264/2022) was amended on 24 July 2024 (effective as of 28 June 2025) to integrate key DSA obligations, including risk assessments, transparency reports, complaint handling, and systemic compliance checks for VLOPs. This amendment formally established the Media Services Council (RPMS) as the national coordinator for digital services and integrated key obligations under the DSA into the Slovak legal framework.[69]

5.2 Institutional Responsibilities

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

Slovakia has designated two competent authorities to enforce the Regulation: the Media Services Council and the Police Force of the Slovak Republic. In the area of terrorist content dissemination, the regulator cooperates closely with foreign partners within global prevention initiatives such as the Christchurch Call, GIFCT, Tech Against Terrorism, and The Global Partnership for Action on Gender-Based Online Harassment and Abuse.[70]

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

The Council for Media Services (RPMS) was designated Slovakia's Digital Services Coordinator under the DSA by the July 2024 amendment. RPMS now monitors compliance, conducts inspections, and can impose fines up to 6 % of global turnover. The RPMS has been an active

[68] Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online (Text with EEA relevance). (online). (cited 2025-09-05). Available at: https://eur-lex.europa.eu/eli/reg/2021/784/oj/eng

[69] Slovakia: Amendments to Media Services Act designating Slovak competent authority and Digital Services Coordinator under the DSA were adopted by National Council. *Digital Policy Alert*. (online). (cited 2025-09-05). Available at:https://digitalpolicyalert.org/event/27021-act-2642022-z-z-on-media-services-and-on-amendments-to-certain-acts-media-services-act-designating-slovak-competent-authorities-and-coordinator-under-the-digital-service-act-dsa-could-was-implemented

[70] Nariadenie o riešení šírenia teroristického obsahu online. *Rada pre mediálne služby*. (online). (cited 2025-09-05). Available at:https://rpms.sk/nariadenie-o-rieseni-sirenia-teroristickeho-obsahu-online

participant in the European network of proto-coordinators and leads a working group focused on systemic risks, demonstrating its proactive preparation for this role.[71]

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

The new responsibilities were assigned to already existing bodies (Police Force of the Slovak Republic mostly). Still, the adoption of the Media Services Act (Act No. 264/2022) and the appointment of the Council for Media Services (RPMS) as the national Digital Services Coordinator (DSC) brought a new, key institutional mechanism (thanks to the DSA). In accordance with Article 21 of the DSA, the RPMS as coordinator certified the first Alternative Dispute Resolution body in Slovakia.[72] This body is the Centre for Alternative Dispute Resolution (CEAH).

- **Status and powers** - CEAH is an independent, private entity certified by the state (RPMS). Its role is to provide out-of-court decisions in disputes between users and platforms. Users whose content was restricted or removed by a platform (e.g., by Meta or TikTok) can turn to CEAH to review whether the platform's decision was in compliance with its terms and conditions and the DSA.

- **Capacity and operation** - The body is in its initial phase of operation. Since its launch in October 2025, it received approximately 100 complaints in the first month. The decision-making apparatus consists of six "arbitrators". Interestingly, CEAH covers submissions from users in both Slovakia and the Czech Republic, suggesting an effective cross-border model.

- **Transparency** - The body's decisions are not currently published as standard, although there is a theoretical possibility of anonymous publication of serious precedent-setting decisions.

---

[71] Slovakia: Amendments to Media Services Act designating Slovak competent authority and Digital Services Coordinator under the DSA were adopted by National Council. *Digital Policy Alert*. (online). (cited 2025-09-05). Available at:https://digitalpolicyalert.org/event/27021-act-2642022-z-z-on-media-services-and-on-amendments-to-certain-acts-media-services-act-designating-slovak-competent-authorities-and-coordinator-under-the-digital-service-act-dsa-could-was-implemented

[72] Article 21 DSA
Out-of-court dispute settlement
...
3. The Digital Services Coordinator of the Member State where the out-of-court dispute settlement body is established shall, for a maximum period of five years, which may be renewed, certify the body, at its request, where the body has demonstrated that it meets all of the following conditions -
(a) it is impartial and independent, including financially independent, of providers of online platforms and of recipients of the service provided by providers of online platforms, including of individuals or entities that have submitted notices;
(b) it has the necessary expertise in relation to the issues arising in one or more particular areas of illegal content, or in relation to the application and enforcement of terms and conditions of one or more types of online platform, allowing the body to contribute effectively to the settlement of a dispute;
(c) its members are remunerated in a way that is not linked to the outcome of the procedure;
(d) the out-of-court dispute settlement that it offers is easily accessible, through electronic communications technology and provides for the possibility to initiate the dispute settlement and to submit the requisite supporting documents online;
(e) it is capable of settling disputes in a swift, efficient and cost-effective manner and in at least one of the official languages of the institutions of the Union;
(f) the out-of-court dispute settlement that it offers takes place in accordance with clear and fair rules of procedure that are easily and publicly accessible, and that comply with applicable law, including this Article.

CEAH's certification is the first practical step by RPMS towards exercising supervision under the DSA. It demonstrates a delegated supervision model where the state regulator (RPMS) will not directly deal with hundreds of thousands of individual content moderation complaints but certifies and delegates this agenda to independent private bodies.

5.3 Obligations for Hosting Service Providers

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

Hosting providers must remove or disable access to terrorist content within one hour of receiving a formal order from competent authorities. This obligation applies to all providers offering services in the EU, regardless of where their main establishment is located.[73]

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

There is the one-hour rule. Failure to comply may result in administrative fines or criminal liability under the amended Slovak Criminal Code, consistent with EU rules. However, official transparency reports published by the Council for Media Services (RPMS) for both 2022 and 2023 show that zero formal one-hour removal orders were issued by the Police Force. In practice, authorities have relied on informal cooperation and notification. For instance, following the 2022 terrorist attack in Bratislava, the RPMS identified 26 URLs hosting the attacker's manifesto and notified the relevant platforms, which subsequently removed the content voluntarily without a formal order being issued. This indicates that the formal legal mechanism is currently being held as a tool of last resort.[74]

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

Under the DSA, as implemented by the amended Media Services Act, Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs) face a comprehensive set of obligations. These include the requirement to conduct and publish annual systemic risk assessments, produce detailed biannual transparency reports on their content moderation activities, appoint an independent compliance officer, and undergo external audits. They must also offer users an option to opt out of personalized content recommendations and are banned from using profiling for targeted advertising to minors or based on sensitive personal data.

---

[73] Gesley, Jenny (2022): European Union: Law on the Obligation to Remove Online Terrorist Content Within One Hour Enters into Force. *Library of the Congress*. (online). (cited 2025-09-05). Available at: https://www.loc.gov/item/global-legal-monitor/2022-08-14/european-union-law-on-the-obligation-to-remove-online-terrorist-content-within-one-hour-enters-into-force/ ; tech against terrorism europe. (online). (cited 2025-09-05). Available at: https://tate.techagainstterrorism.org/the-tco

[74] 2022 Annual transparency report on activities of the Council for Media Services under Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online. (online). (cited 2025-09-05). Available at: https://rpms.sk/sites/default/files/2023-04/TCO_report_CMS.pdf ; 2023 Annual transparency and monitoring report on activities of the Council for Media Services under Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online. (online). (cited 2025-09-05). Available at: https://rpms.sk/sites/default/files/2024-04/2023_TCO_report_CMS.pdf

5.4 Notification and Removal Procedures

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

Authorities initiate a judicial order based on identifiable terrorist content. When issuing a removal order, the competent authority (the Police Force) must provide a formal document that includes a detailed statement of reasons explaining why the specific content is considered terrorist in nature under the regulation. The order must also contain precise information to allow the provider to locate the content, such as the exact URL, and if necessary, additional details like screenshots. The order must also inform the provider about available redress mechanisms. Providers must comply within one hour.

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

In Slovakia, removal orders for terrorist content are subject to a post-removal judicial review by court. Both hosting service providers and content providers have the right to an effective remedy to challenge a removal order before the national courts. This means the court assesses the legality and proportionality of the order after the content has already been taken down. While this serves as a crucial safeguard against unconstitutional prior restraint, its post hoc nature means the content is suppressed during the review period, and the immediate impact on speech has already occurred even if the order is later overturned.[75]

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

Platforms must offer clear reporting channels. If a platform decides to remove or restrict the reported content, it must provide the affected user with a clear and specific statement of reasons for its decision. The Council for Media Services (RPMS), as the DSC, is responsible for overseeing platform compliance with these requirements and ensuring the guidelines are followed. RPMS thus ensures compliance, it may conduct inspections, and can impose penalties according to the DSA framework.

5.5 Sanctions and Penalties

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

Under the national implementation, Slovak law empowers courts and authorities to impose administrative fines on hosting providers failing to remove terrorist content within the one-hour deadline. While maximum amounts aren't specified, the Criminal Code amendments allow substantial penalties, including potential personal liability.[76]

---

[75] National courts and other non-judicial bodies. *European e-Justice Portal*. (online). (cited 2025-09-05). Available at: https://e-justice.europa.eu/topics/your-rights/fundamental-rights/where-can-i-get-help/list-relevant-courts-and-bodies/national-courts-and-other-non-judicial-bodies/sk_en

[76] Regulation on addressing the dissemination of terrorist content online. *Rada pre mediálne služby*. (online). (cited 2025-09-05). Available at: https://rpms.sk/en/regulation-addressing-dissemination-terrorist-content-online; Node. *Council for media services*. (online). (cited 2025-09-05). Available at: https://rpms.sk/en/node

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

Slovakia enforces the DSA using the amended Media Services Act (No. 264/2022). For serious violations – such as not conducting risk assessments or mishandling transparency reporting – fines can reach up to 6 % of the global annual turnover of a service provider.

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

To date, there have been no publicly announced penalties imposed in Slovakia under either the TCO Regulation or the DSA. However, the RPMS has been active under its broader media services mandate. E.g., in January 2025 RPMS issued sanctions, including a warning and financial penalty to TV Markíza related to potential breaches of objectivity. On the other hand, it halted proceedings against Topky.sk after questionable content was removed. Finally it issued warnings to TV Joj and a €1,000 fine was imposed upon Dajto for non-compliance with record-keeping rules.[77]

5.6 Scope and Application

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

Yes. All platforms available in Slovakia must comply with the one-hour terrorist takedown mandate. However, obligations under the DSA vary: Very Large Online Platforms (VLOPs) face full-scale compliance obligations (risk analyses, transparency, compliance officer). Smaller platforms and start-ups are subject to notice-and-action duties but benefit from a lighter regulatory regime (such as conducting systemic risk assessments and appointing a compliance officer, although they must still comply with baseline duties like having effective notice-and-action mechanisms).[78]

Does your country apply any specific exemptions or streamlined procedures for non-profit platforms, academic repositories, or other niche services?

Slovakia adopts the EU principle granting partial exemptions to non-profit platforms, academic repositories, and non-commercial tools—they are exempt from risk assessments and compliance personnel requirements, though they must still maintain notice-and-action protocols.[79]

---

[77] Hill, Jeremy (2025): Media Services Council imposes fines and halts proceedings. *Rádio Slovakia international*. (online). (cited 2025-09-05). Available at: https://enrsi.stvr.sk/articles/news/389589/media-services-council-imposes-fines-and-halts-proceedings

[78] L/R/P advokáti (2025): New cybersecurity requirements impact energy sector. *The Slovak spectator*. (online). (cited 2025-09-05). Available at: https://spectator.sme.sk/business/c/new-cybersecurity-requirements-impact-energy-sector; Freud, Gideon (2022): Mapping Internet Regulations: Online Terrorist Content. *Active Fence*. (online). (cited 2025-09-05). Available at: https://www.activefence.com/blog/mapping-internet-regulations-terrorist-content/

[79] Node. *Council for media services*. (online). (cited 2025-09-05). Available at: https://rpms.sk/en/node; Accessibility statement. Council for media services. (online). (cited 2025-09-05). Available at: https://rpms.sk/en/accessibility-statement

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 publicly known lawsuits have challenged Slovakia's implementation of the one-hour terrorist content removal mandate.

What arguments—constitutional, procedural, or otherwise—have been raised in these challenges?

While no formal litigation has occurred, civil society organizations such as VIA IURIS have warned that the one-hour rule may be disproportionate and potentially conflict with constitutional rights (Art. 26) or procedural safeguards.

5.8 Transparency and Reporting

Do authorities or platforms publish reports on the volume of terrorist content removed under Regulation (EU) 2021/784?

The Council for Media Services (RPMS) publishes annual transparency reports detailing the number of removal orders issued and compliance statistics, as stipulated under Articles 8 and 21 of the Regulation 2021/784. However, the reports for both 2022 and 2023 stated that zero formal one-hour removal orders were issued and consequently, no content was formally removed under this specific legal mechanism.[80]

Under the DSA, what transparency requirements exist for service providers (e.g., content moderation reports)?

All VLOPs must publish annual Transparency Reports, including data on content moderation, add handling, and systemic risk assessments.[81]

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

Information is publicly available via RPMS's website and EU-level DSA Transparency Centre in Slovak and English (DSA Transparency Database), allowing access by the public and watchdog NGOs.[82]

---

[80] 2022 Annual transparency report on activities of the Council for Media Services under Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online. (online). (cited 2025-09-05). Available at: https://rpms.sk/sites/default/files/2023-04/TCO_report_CMS.pdf ; 2023 Annual transparency and monitoring report on activities of the Council for Media Services under Regulation 2021/784 of the European Parliament and of the Council on addressing the dissemination of terrorist content online. (online). (cited 2025-09-05). Available at: https://rpms.sk/sites/default/files/2024-04/2023_TCO_report_CMS.pdf

[81] Parliamentary Monitor. (online). (cited 2025-09-05). Available at: https://www.eumonitor.eu/9353000/1/j4nvhdfcs8bljza_j9vvik7m1c3gyxp/vmaqmq3o48rp

[82] DSA Transparency Database. *European Commission*. (online). (cited 2025-09-05). Available at: https://transparency.dsa.ec.europa.eu/; Transparency Center. *Meta*. (online). (cited 2025-09-05). Available at: https://transparency.meta.com/reports/regulatory-transparency-reports/

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?

Slovakia is an active participant in the EU's cooperative enforcement architecture. The RPMS is a full member of the European Board for Digital Services, which ensures the consistent application of the DSA across the Union. For terrorist content, national authorities are part of the EU Rapid Takedown Network.

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

Europol's Terrorist Content Analytics platform, DSA Coordinator Network, and Digital Services Board regularly share reports and hold exchanges with Slovak authorities through RPMS.

Europol operates the PERCI platform, a secure channel for issuing and processing removal orders across borders.

Eurojust facilitates and coordinates complex cross-border judicial investigations related to serious online crime, providing funding and strategic support for Joint Investigation Teams. The European Board for Digital Services also serves as a key forum for exchanging best practices among national coordinators.

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

In May 2022, Slovak and Czech authorities collaborated closely – under the coordination of Eurojust and with support from Europol and U.S. law enforcement – in a major operation against a suspected far-right extremist operating online. The suspect was accused of: Inciting the overthrow of democratic institutions, sharing instructions for manufacturing weapons, explosives, mines and distributing far-right propaganda and extremist content. It is a demonstration of cross-border cooperation under the DSA Regulation and the Terrorist Content Regulation, applying traditional criminal justice tools in the online sphere. The case involved online dissemination of terrorist content and weapon-making instructions, connecting cyber investigation with physical enforcement.[83]

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?

VIA IURIS warned that the one-hour takedown rule could lead to excessive removal of lawful content, potentially contravening constitutional freedoms. There are concerns that the fast removal regimes under Regulation (EU) 2021/784 and the DSA could lead platforms to err on the side of removal, over-censoring content to avoid penalties. A 2024 study found that platforms may

[83] Terrorism. *EUROJUST*. (online). (cited 2025-09-05). Available at: https://www.eurojust.europa.eu/annual-report-2022/key-cases-and-developments/terrorism; EuropaWire PR Editor (2023): Eurojust Coordinates Crackdown on International Online Fraud Network. *EUROPAWIRE*. (online). (cited 2025-09-05). Available at: https://news.europawire.eu/eurojust-coordinates-crackdown-on-international-online-fraud-network/eu-press-release/2023/11/08/09/53/57/124594/

be "over-removing content to avoid regulatory penalties," and the broad definitions of hate speech exacerbate this risk.[84]

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

The DSA itself includes strong safeguards: all removal requests must include clear reasoning, and users must receive explanation and transparency reports. In Slovakia, the amendments to the Media Services Act designate the Council for Media Services as the national Digital Services Coordinator (DSC). This body is empowered to enforce compliance while respecting fundamental rights under the EU Charter and GDPR. The Media Services Act includes proportionality principles, mandatory human oversight, internal appeals, and judicial review, ensuring protection of expression and data rights.

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

Content creators or users can file a written objection with the authority against the issued penalty order within 15 days of its delivery. In Slovakia, the DSC (Council for Media Services) can receive user complaints directly, conduct investigations, and impose sanctions while respecting procedural fairness. An end user may also seek judicial review under the EU Charter via Slovak courts.

5.11 Comparisons with Other Jurisdictions

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

Slovak lawmakers and regulators have considered implementation models from neighbouring Member States, especially the Czech Republic, Austria, and Germany. These jurisdictions' approaches – such as the designation of trusted flaggers, transparency measures, and regulatory powers – have informed Slovakia's own national framework.

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

While the core obligations are harmonized at the EU level, there are subtle differences in institutional design. A notable distinction is that Slovakia has centralized the role of the Digital Services Coordinator within its existing media authority (RPMS). This creates a more streamlined structure compared to some neighbors, like the Czech Republic, where the DSC is the national telecommunications authority (CTU), or Poland, where responsibilities are to be split between the President of the Office of Electronic Communications (UKE) and the President of the Office of Competition and Consumer Protection (UOKiK). Austria's DSC is the Communications Authority (KommAustria), and Hungary's is the National Media and Infocommunications Authority (NMHH), an appointment that has raised concerns among some Members of the European Parliament regarding its independence.[85]

---

[84] Portaru, Adina (2025): How the EU Digital Services Act (DSA) Affects Online Free Speech in 2025. *ADF International*. (online). (cited 2025-09-05). Available at: https://adfinternational.org/commentary/eu-digital-services-act-one-year

[85] Cunningham, Francine – Sasdelli, Paolo (2024): Which countries have appointed their Digital Services Coordinators under the DSA?. *Bird&Bird*. (online). (cited 2025-09-05). Available at: https://www.twobirds.com/en/insights/2024/global/which-countries-have-appointed-their-digital-services-coordinators-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?

In Slovakia, the .sk country-code top-level domain (ccTLD) is administered by SK-NIC, a.s., a private joint-stock company operating the registry.[86]

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

SK-NIC obtained administration of .sk through historic delegation and continued recognition by IANA/ICANN since its establishment, following standard cooperative agreement with the Ministry of Finance of the Slovak Republic.[87]

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

The role of SK-NIC, a.s. as the administrator of Slovakia's .sk domain is governed by a combination of international delegation frameworks, national regulatory frameworks, and internal policies which consists of: ICANN Delegation, Cooperation Agreement with the Slovak Government, SK-NIC Terms & Conditions and Official "Rules" and Slovak National and EU Law Compliance. Cooperation Agreement establishes a hybrid governance model, creating a commission with government, internet community, and SK-NIC representatives to oversee domain management policies.[88]
The actual technical, administrative, and contractual role of the administrator of the national .sk domain (SK-NIC, a.s.) and its cooperation with state authorities in suspending domains based on court orders or statutory requirements is actually only a minor one.

The analysis of the disinformation ecosystem namely shows that the information war overwhelmingly does not take place on websites with the national .sk domain. Tools like domain blocking are almost irrelevant for threats such as the 2023 deepfake incident, disseminated via the global applications Telegram and Facebook, or for algorithmically amplified content on TikTok, which the SIMODS study identified as the main vector for spreading disinformation in Slovakia.[89]

The role of SK-NIC is thus technically and administratively important for the management of the national internet space, but in terms of the real fight against modern disinformation, its significance today is marginal. The regulatory focus has definitively shifted from controlling the national domain registry (SK-NIC) to enforcing rules on global algorithmic platforms (RPMS and DSA).

---

[86] SK-NIC. *ICANNWiki*. (online). (cited 2025-09-05). Available at: https://icannwiki.org/SK-NIC
[87] Country code top-level domain. *ICANNWiki*. (online). (cited 2025-09-05). Available at: https://icannwiki.org/Country_code_top-level_domain
[88] SK-NIC. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/about-us/; Rules. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/documents/rules/
[89] (cited 2025-09-05). Available at: https -//demagog.sk/prva-rozsiahla-europska-studia-odhalila-kde-sa-na-socialnych-sietach-siri-najviac-nepravdivych-informacii

6.2 Responsibilities and Mandate

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

The core functions of SK-NIC, a.s. are technical and administrative. They include managing the domain name registration system, operating the Domain Name System (DNS) for the.sk zone, enforcing its registration policies, and administering an Alternative Dispute Resolution (ADR) process for domain name conflicts.[90]

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

No. SK-NIC's mandate is technical and administrative only – it does not regulate or oversee website content under .sk domains. This aligns with its mandate as Slovakia's ccTLD operator, as defined by its ICANN/IANA delegation and internal policies, which focus exclusively on domain management, without legal authority over web content. This position was affirmed in a court case involving the domain dpdkurier.sk, where it was ruled that SK-NIC could not be held liable for trademark infringement by a domain holder, only to act as a technical executor of a court order directed at the infringer.[91]

6.3 Registration Policies

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

Registrants must comply with the official SK-NIC registration policy, which may include residency or trademark protection requirements. Specific eligibility rules and guidelines are publicly available.[92]

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

Some domain names (e.g. government domains or specific sectors - gov.sk) may be subject to special restrictions or reserved by law or regulator and thus are unavailable for general public registration.

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

SK-NIC provides publicly available documents on its website outlining procedures for registration, supported by dispute-resolution and domain revocation policies.[93]

---

[90] How to become a Registrar of .sk domain. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/how-to-become-a-registrar-of-sk-domain/

[91] Lazur, Ján – Nagy, Zoltán (2018): Slovakian top-level domain authority (.sk) not individually liable for IP infringement. TaylorWessing. (online). (cited 2025-09-05). Available at: https://www.taylorwessing.com/en/insights-and-events/insights/2018/10/slovakian-toplevel-domain-authority-sk-not-individually-liable-for-ip-infringement

[92] How to become a Registrar of .sk domain. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/how-to-become-a-registrar-of-sk-domain/

[93] Rules. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/documents/rules/

6.4 Dispute Enforcement

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

SK-NIC can revoke or suspend domains when policy violations occur—this includes non-payment, infringement, outstanding court orders, or abuse of domain names. Crucially, suspension can also occur in compliance with a binding and lawful court order.[94]

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)?

SK-NIC cooperates with Slovak authorities (e.g. NBÚ) and provides assistance (such as suspensions) in response to court decisions or lawful requests. These requests must be submitted properly, registered, and then SK-NIC responds accordingly.[95]

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

SK-NIC explicitly states that to obtain hidden or historical personal data, authorities must send a standardized formal request (on paper or secure electronic form). This process is detailed in SK-NIC's FAQ and Terms & Conditions. Additionally, SK-NIC entered a formal Cooperation Agreement in 2006 with the Slovak government, outlining oversight roles and structured governance in the National Domain Management Commission.[96]

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

A significant case occurred following Russia's 2022 invasion of Ukraine. After the Slovak parliament passed emergency legislation to enable the blocking of disinformation websites, SK-NIC, a.s. issued a public statement affirming its readiness to "respond immediately" to deactivation requests from competent authorities concerning domains identified under this new law, demonstrating its capacity to act as an enforcement tool when a clear legal predicate is established by the state.[97]

---

[94] FAQ: Registrar. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/faq-en/registrar/#how-to-cancel-registrars-account

[95] FAQ: Official. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/faq-en/official/#when-will-sk-nic-block-the-domain-in-case-of-adr-proceeding; FAQ: Official. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/faq-en/official/#how-can-the-law-enforcement-authority-request-to-receive-hidden-or-historical-data-non-public-information

[96] (2018): SK-NIC acquisition process has been closed. SK-NIC´s new strategic investor and owner is UK company CentralNic. *British Chamber of Commerce in the Slovak Republic*. (online). (cited 2025-09-05). Available at:https://britcham.sk/infrastructure-investment-boom-predicted-for-cee-nations-on-the-rise-3-2/

[97] (2022): Statement of SK-NIC, a.s. on deactivation of the so-called disinformation domains / websites. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/en/statement-of-sk-nic-a-s-on-deactivation-of-the-so-called-disinformation-domains-websites/

6.6 Transparency and Accountability

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

SK-NIC's dispute resolution policy includes mechanisms allowing registrants to appeal administrative decisions or suspensions. Domain holders can challenge decisions through the official Alternative Dispute Resolution (ADR) process administered by SK-NIC, a.s. and, if the outcome is unsatisfactory, they can ultimately pursue the matter through the national court system.[98]

6.7 Economic and Market Considerations

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

Domain registration fees for .sk are set by SK-NIC independently, without direct government regulation, though subject to market norms and internal pricing policies.[99]

[98] Hutko (2010): The First Supreme Court Decision on Domain Names. *Tech notes*. (online). (cited 2025-09-05). Available at:https://husovec.eu/2010/10/the-first-supreme-court-decision-on-domain-names/; Domain Name Monitoring Detect brand and trademark infringing domain names fast. *Webnames corporate*. (online). (cited 2025-09-05). Available at: https://webnamescorporate.com/brand-protection/domain-monitoring/#:~:text=Litigation:%20If%20the%20above%20processes%20fail%2C%20litigation,another%20party%20should%20rightfully%20belong%20to%20them.

[99] Nové .sk domény budú opäť dočasne lacnejšie. *DSL.sk*. (online). (cited 2025-09-05). Available at: https://www.dsl.sk/article.php?article=28507; Finálne znenie pravidiel a nový cenník. *SK-NIC*. (online). (cited 2025-09-05). Available at: https://sk-nic.sk/finalne-znenie-pravidiel-a-novy-cennik/

7
INDEPENDENT OVERSIGHT MECHANISMS

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?

Slovakia has Public Defender of Rights (Ombudsman) who was established under Article 151a of Slovakia's Constitution (and Act No. 564/2001 Coll.), protecting fundamental rights against public administration bodies. Also, there is the Slovak National Centre for Human Rights (SNCHR) – the national human rights institution and equality body, created by Act No. 308/1993 Coll., accredited B-status by ENNHR.[100]

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

Ombudsman was established as a constitutionally independent body (Art. 151a) established by the force of law; the ombudsperson is being appointed by Parliament for one-time renewable 5-year term, fully autonomous from government/lawmaking bodies. Slovak National Centre for Human Rights (SNCHR) was founded by statute of the Parliament; its B-status is indicating recognized but limited independence under the Paris Principles.

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

Neither body has explicit legal mandates covering digital rights, online freedom of expression, or online content regulation – they focus broadly on human rights violations by public bodies. They may, however, address internet-related issues analogously if affecting privacy, freedom of expression, or discrimination.

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)?

Ombudsman can investigate alleged human-rights violations by public administration, including online aspects like data retention, privacy infringements, or censorship by state agencies. Slovak National Centre for Human Rights (SNCHR) handles anti-discrimination complaints and broader human rights abuses, including digital privacy and equality online, online hate speech, and ensuring equal access to digital services.[101]

[100] Slovak National Centre for Human Rights (2022): Slovak National Centre for Human Rights - State of the Rule of Law in Europe in 2022 - Reports from National Human Rights Institutions – Slovakia. *Europa.eu*. (online). (cited 2025-09-05). Available at: https://www.eesc.europa.eu/en/sections-other-bodies/other/group-fundamental-rights-and-rule-law/frrl-trends-eu-member-states/slovak-national-centre-human-rights-state-rule-law-europe-2022-reports-national-human

[101] Public Defender of Rights (Ombudsman, Ombudsperson). *Human Rights Guide*. (online). (cited 2025-09-05). Available at: https://www.humanrightsguide.sk/en/themes/organisations-that-can-help-you/state-institutions/public-defender-of-rights-%28ombudsman-ombudsperson%29

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

Ombudsman issues non-binding recommendations. He can propose amendments to laws and challenge legislation before the Constitutional Court but cannot enforce binding decisions. Slovak National Centre for Human Rights provides policy recommendations, reports, and can litigate to enforce anti-discrimination law; still, it lacks binding enforcement powers. Their power lies in public reporting and persuasion.

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

Ombudsman selects cases based on legal merit, seriousness of violations, and prevalence. He can act independently (ex officio). Slovak National Centre for Human Rights monitors systemic issues; prioritizes based on discrimination trends, alignment with international obligations, or rule-of-law monitoring.

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)?

Affected people can contact ombudsman via online/email, their website, postal mail, or in-person. No fees are collected, both Slovak and other languages can be used. Likewise, the Slovak National Centre for Human Rights provides legal help/support services in case of discrimination complaints; it can be contacted via email or in-person.
This mandate can be supplemented with a concrete output of SNCHR's activity in the digital sphere - the already mentioned monitoring report “Hate Language on Political Facebook Profiles” from 2023, which is a direct fulfillment of the SNCHR's mandate in monitoring the protection of human rights online.

The most significant change in the area of supervision is the emergence of a new, hybrid architecture that complements traditional supervision (SNCHR) and self-regulation (Press and Digital Council of the SR). These are:

a) NGO contracted by a private platform

The Demagog.sk platform gained a formalized and influential role. It became an official partner of the Meta company (operator of Facebook and Instagram) within the “3rd party fact-checking” program.[102] Under this cooperation, Demagog.sk performs content evaluation and commits to issuing transparent reports on its activities. This is a model where a civil society organization (NGO) performs factual content oversight based on a contractual mandate from a multinational private company.

b) Private body certified by the state

[102] (cited 2025-09-05). Available at: https -//demagog.sk/meta-na-slovensku-pridava-demagog.sk-medzi-partnerov-do-svojho-programu-overovania-faktov%C2%A0

As already mentioned, the establishment of CEAH represents the second hybrid model. Here, a private body (CEAH) gains the authority for dispute resolution (oversight over platform decisions) based on official certification from the state regulator (RPMS).

Oversight of internet content in Slovakia is therefore no longer monolithic. It is fragmenting into a new, complex three-tiered architecture:

- **State supervision** - RPMS (DSA oversight), SNCHR (human rights).
- **Self-regulation** - Press and Digital Council of the SR.
- **Hybrid/Delegated supervision** - CEAH (private certified by the state) and Demagog.sk (NGO contracted by a private platform).

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

These mechanisms are free of charge, with online and multilingual access. Interpretation costs at the official (state) level are covered by the state.[103]

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

The remedies take primarily the forms of "soft power." Ombudsman issues recommendations, law amendment proposals, court referrals to Constitutional Court, and public reports. Crucially, the Ombudsman also possesses the "hard power" to refer legislation directly to the Constitutional Court for a binding review of its constitutionality. Slovak National Centre for Human Rights provides legal representation, equality/inclusion measures, policy recommendations, and can initiate anti-discrimination court actions.[104]

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?

Ombudsman and Slovak National Centre for Human Rights both may be formally consulted during legislative drafting; they can submit proposals, opinions, or challenge legislation like data retention or media laws.

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

They issue formal opinions and recommendations. However, because Ombudsman rulings are non-binding, the government may ignore them, as occurred with past reports, particularly when they conflict with the political agenda of the ruling majority.

[103] Public Defender of Rights (Ombudsman, Ombudsperson). *Human Rights Guide*. (online). (cited 2025-09-05). Available at: https://www.humanrightsguide.sk/en/themes/organisations-that-can-help-you/state-institutions/public-defender-of-rights-%28ombudsman-ombudsperson%29

[104] Slovakia: Business and human rights. *European e-Justice*. (online). (cited 2025-09-05). Available at: https://e-justice.europa.eu/topics/your-rights/fundamental-rights/business-and-human-rights/sk_en

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

Not yet, however, in late 2024, Róbert Dobrovodský, the Public Defender of Rights (Ombudsman), formally filed a request with the Constitutional Court to review a new amendment to Slovakia's Act on Free Access to Information. He argued that provisions allowing public authorities (e.g., ministries, municipalities) to charge fees for requested information threatened to hinder citizens' rights. He emphasized that if the law took effect on March 1, 2025, it would degrade the high standard of information access Slovakians had enjoyed for the previous 24 years.[105]

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?

A group of Slovak MPs, supported by the European Information Society Institute (EISi), filed a complaint challenging the national implementation of the EU Data Retention Directive as disproportionate and unconstitutional. In its ruling PL. ÚS 10/2014, the Constitutional Court struck down the national laws that implemented the EU's Data Retention Directive. The Court found that the blanket, preventative retention of telecommunications traffic and location data for all citizens constituted a disproportionate and unconstitutional interference with the right to privacy guaranteed by the Slovak Constitution and the ECHR. The ruling effectively ended the practice of mass data retention in Slovakia and stands as a landmark victory for privacy rights, achieved through the mechanism of constitutional litigation.[106]

This strategy continues to be employed. In late 2024, the Public Defender of Rights, Róbert Dobrovodský, formally filed a request with the Constitutional Court to review a new amendment to the Act on Free Access to Information, as mentioned above, demonstrating the ongoing use of constitutional litigation as the primary tool for protecting fundamental rights against legislative encroachment.

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

The Constitutional Court's rulings effectively ended mass data retention in Slovakia, reinforcing citizens' privacy and aligning national law with EU standards.

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

The primary challenges faced by these institutions are insufficient financial and human resources, which limits their capacity to take on complex, technically demanding digital rights cases. Additionally, Ombudsman's recommendations are of an advisory nature only; they lack binding

[105] TASR (2018): Ombudsman sa obráti na Ústavný súd kvôli novele infozákona. *SME*. (online). (cited 2025-09-05). Available at:https://domov.sme.sk/c/23422755/ombudsman-sa-obrati-na-ustavny-sud-kvoli-novele-infozakona.html

[106] ERDI (2014): Slovak Constitutional Court suspends data retention legislation. *ERDi*. (online). (cited 2025-09-05). Available at:https://edri.org/our-work/slovak-constitutional-court-suspends-data-retention-legislation/; (2012): Slovakian data retention law faces challenge before Constitutional Court. *STATEWATCH*. (online). (cited 2025-09-05). Available at: https://www.statewatch.org/news/2012/october/slovakian-data-retention-law-faces-challenge-before-constitutional-court/

authority and are often being ignored by Parliament or executive bodies due to political pressure or bias. Ombudsman's involvement in the data retention process was largely indirect and supporting, reflecting institutional limits in initiating litigation or interventions on their own.

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 academia see Ombudsman as a useful check, though too weak in enforcement, especially on digital rights issues since his lack of binding authority.

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

Critiques include lack of binding power, insufficient financial/human resources, and occasionally perceived political bias in Parliament ignoring reports.

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

Dependence on the state budget might limit the capability of Ombudsman's office. Political pressure could undermine the ability to act independently.

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?

EU Digital Services Act and growing digital challenges fuel calls to strengthen oversight, possibly by expanding mandates or updating laws. However, as of today, there are no concrete reforms underway.

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

Emerging tech like AI moderation increases the need for specialized oversight. While stakeholder discussions exist (e.g. via experts like B. Bukovská in EU forums), no new Slovak institutions have been created. The 2023 election deepfake incident and the impending implementation of the EU AI Act have highlighted the inadequacy of existing analog-era mandates to address complex digital threats, fueling calls from experts and civil society for more expert and technically proficient oversight bodies.

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

There are no formal proposals to create new digital rights bodies, though stakeholders advocate for dedicated digital rights commissioner offices or stronger NHRI capacities.

7.8 Comparisons and Best Practices

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

The Slovak National Centre for Human Rights participates in the European Network of National Human Rights Institutions (ENNHRI) and EU rule-of-law mechanisms, and follows the Council of Europe and UN standards.[107]

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

The Ombudsman occasionally issues special reports and submits cases to the Constitutional Court, while the Slovak National Centre for Human Rights contributes to rule-of-law reporting and monitors digital rights annually. These activities could serve as valuable templates for other countries.

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

While compliant with CoE and UN Charter, Slovakia's Slovak National Center for Human Rights lacks full NHRI "A-status" independence and enforcement power – it is thus positioned somewhere between regional minimums and best-in-class models for national human rights institutions and highlighting a key area for potential improvement.[108]

[107] Slovak National Centre for Human Rights (2022): Slovak National Centre for Human Rights - State of the Rule of Law in Europe in 2022 - Reports from National Human Rights Institutions – Slovakia. *Europa.eu*. (online). (cited 2025-09-05). Available at: https://www.eesc.europa.eu/en/sections-other-bodies/other/group-fundamental-rights-and-rule-law/frrl-trends-eu-member-states/slovak-national-centre-human-rights-state-rule-law-europe-2022-reports-national-human

[108] NHRI accreditation status and mandates - update 2024. *European Union Agency for Fundamental Rights*. (online). (cited 2025-09-05). Available at: https://fra.europa.eu/en/publication/2024/nhri-accreditation-status-and-mandates-update-2024?page=1#read-online