

Case study: Slovakia

ANDREJ ŠKOLKAY

1. Introduction

This chapter explores how Slovakia tackled online disinformation from regulatory perspective and analyses the operating practices in place during the years 2018–2023. It also covers regulatory changes (following Digital Services Act) impacting social media platforms, video sharing platforms, and search engines, resulting from the media regulator’s expanding competences from the summer of 2024 onward (some of which have been in effect only since June 2025).

It should be noted that the strategic and tactical efforts for combating disinformation were rather diverse and became increasingly intensive. However, some of them were also arguably unconstitutional. Moreover, it remains questionable whether authorities can or cannot actually block websites as of 2024. The legislation, amended by Parliament in 2022, is rather confusing in that regard. The fact is that the state has not blocked any website on the basis of broadly understood political arguments, since 2022 (as of July 2024). The exception is a pan-European decision taken to block certain Russian websites, as will be discussed later.

This chapter offers an overview of the key regulations, key actors and key regulatory outputs (including drafts and temporary regulations which were only in force for a brief time).

Why was tackling online disinformation seen as a key issue to address in Slovakia? The blocking of some local online news and current affairs outlets was seen as controversial from a constitutional perspective (freedom of speech and of the press) by some lawyers and NGOs. Within this context, it could also be said that the causes of relative popularity and relative ease of penetration in society of disinformation and fake news/hoaxes, selection of regulatory approaches how to tackle this issue, were by and large based on incorrect assumptions. Specifically, it was assumed that online disinformation is capable of having a significant impact on the population at large. However, such a claim – that propaganda can always have immediate and direct impact on humans without any pre-conditions – is not supported by almost a century of research into propaganda.¹ Of course, this does not contradict the idea that “small effects suddenly matter a great deal”.² This issue is illustrated further on an example of fake video used in the campaign before the 2023 general elections.

It should be acknowledged that fake news and hoaxes are a political problem, especially for a society that is inclined to believe in conspiracy theories. In fact, in the region, Slovak

¹ HAMID (2022); ANDERSON (2021); URSPRUNG (1994).

² SANDER VAN DER LINDEN: Psychological weapons of mass persuasion. *Scientific American*, 10 April 2018. <https://www.scientificamerican.com/article/psychological-weapons-of-mass-persuasion/>

respondents are the most likely to believe in conspiracy theories. Sixty percent of respondents believed that world events are decided by secret groups and associations that strive to create a totalitarian world government. Half believe that the Jews have too much power and covertly control the world. More than half the Slovak population believes that its values are threatened by the USA. Almost two thirds of respondents (also the highest figure in the region, expressed their readiness to give up their freedoms in exchange for other benefits. Respondents who were prone to believe conspiracy and disinformation narratives also tended to prefer autocratic leaders and were more willing to give up their democratic freedoms in exchange for other benefits. Such as improving the financial situation, security, or preserving traditional values.³

It has already been established in scientific literature that political discussions on social media often lead to (greater) polarisation (echo chambers) and, especially on Facebook, to (even more) anger.⁴ It is also the case that ‘alternative media’⁵ are most often accessed via Facebook.⁶

Considering these points, it should not be surprising that trust in the traditional media and authorities is low overall, among a large part of the public. In the years 2017–2023, overall trust in the media oscillated below 27%. Respondents expressed higher trust (37%) in the media that they followed. Only two monitored media – public service media *RTVS* (*Radio and Television of Slovakia*, now *Slovak Television and Radio* or *STVR*), and news television *TA3*, reached over 50% trust.⁷ However, other research suggested that these two media channels attained significantly higher levels of trust (absolute trust and more likely trusted) – with trust levels of 74% and 71% respectively.⁸ In a similar vein, two thirds of both online users and offline users noticed fake news in the sources they followed.⁹

Some other media, like online only news portal *aktuality.sk* (*Hot News*), business newspaper *Hospodárske noviny* (*Business Newspaper*), radio *Rádio Express*, commercial *TV Joj*, and regional and local newspapers, reached trust levels of almost 50%, according to one study.¹⁰ In another study, they reached over 50% trust level (absolute trust and more likely trusted).¹¹ However, it is doubtful that “Very low trust (27%) in news in general reflects decades of interference by business and political leaders”,¹² as the authors of the report claimed. In particular, there was no direct business or political interference in public service media or the majority of other major media outlets over the last decade. In fact, there are other more plausible explanations available for explaining low trust in the media. In addition to those already mentioned, this include the fact that trust in political institutions is

³ HAJDU–KLINGOVÁ (2020)

⁴ OSMUNDSEN – BANG PETERSEN – BOR (2021), SPOHR (2017), ANSTEAD (2021).

⁵ There are many definitions of alternative media. However, in local discourse these are understood mostly normatively negatively, as those outlets (almost exclusively online) that do not follow journalistic standards. Furthermore, Facebook bans most controversial alternative media outlets.

⁶ ŠTEPANOVIČ (2021)

⁷ CHLEBCOVÁ HEČKOVÁ – SMITH (2023)

⁸ 2MUSE (2021)

⁹ 2MUSE (2021)

¹⁰ CHLEBCOVÁ HEČKOVÁ – (2023)

¹¹ 2MUSE (2021)

¹² CHLEBCOVÁ HEČKOVÁ – SMITH (2023)

low in general, with maximum trust found in case of local governments (trusted by 36%).¹³ For the media, less than 20% of respondents believed that media activities are somehow useful for society.¹⁴ Moreover, 61% of respondents thought that it was complicated for them to check whether they follow trustworthy news.¹⁵ There is also an issue with the liberal attitude of the key mainstream and agenda-setting media, given that the majority of population is ideologically and culturally more conservative in many respects.¹⁶ This is related to a human need to share politically congruent information. It could be that a key turning point is when the media by and large failed to cover large-scale corruption – which could be seen as an early phase of state capture.¹⁷

There is also overall low trust in society. About 10% of Slovaks – the lowest results among OECD members – believed they can trust others in 2014. The average for positive answers for OECD member countries was 36%.¹⁸ However, more recent data has suggested that general interpersonal trust has been stagnant for a long time – it has been oscillating around 23% for the last three decades. Moreover, trust in (some) institutions was much higher.¹⁹ Pro-Russian attitude (e.g. delivery of weapons to Ukraine is more often seen as provocation towards Russia, rather than help for Ukraine)²⁰ can also be explained by deeper and long-term cultural factors, as opposed to successful Russian propaganda.²¹

As a result of the above-mentioned deeper and long-established social-cultural factors and trends, ‘alternative’ media or ‘alternative sources’ in general, are popular among certain relatively limited segments of population. Additionally – and perhaps more importantly – dissemination of disinformation is widespread via social media. As mentioned above, messages produced by ‘alternative media’ are most often accessed via Facebook.²² Moreover, with the exception of *Zem & vek* (The Earth & Age) monthly journal, alternative media are not distributed in printed format (except for occasionally published special issues, for example, *Hlavné správy* – The Headlines or the Main News). There is a ratio about 1:2 of those who prefer ‘alternative’ media (such as *Hlavné správy*, *Zem a Vek*, *Slobodný vysielateľ*, *Infovojna*) and ‘standard’ media (such as *SME [We Are]*, *Denník N [Newspaper N]*, *Aktuality [Hot News]*).²³ However, this means that about 13% of the population follows alternative media a few times a week; while almost 28% of the population prefers standard media. Yet, at the

¹³ Ako sa máte, Slovensko? Dôvera v inštitúcie 2. [Trust in institutions]. (Survey), *Ako sa máte, Slovensko?* <https://www.akosamateslovensko.sk/tema/dovera-v-institutcie/>

¹⁴ Ibid. It could be said that the loss of trust in ‘mainstream’ media is a global trend, however, these figures are still higher than those in the USA. Megan BRENAN: Media Confidence in U.S. Matches 2016 Record Low. Gallup, 19 October 2023. <https://news.gallup.com/poll/512861/media-confidence-matches-2016-record-low.aspx>

¹⁵ 2MUSE (2021)

¹⁶ ŠKOLKAY (2022)

¹⁷ ŠKOLKAY (2018)

¹⁸ Spectator staff: Slovaks are among the least trusting people. The Slovak Spectator, 2 March 2017. <https://spectator.sme.sk/c/20473017/slovaks-are-among-the-least-trusting-people.html>

¹⁹ DEKK Institute: *Trends of [dis]trust 2023*. Bratislava, DEKK Institute, 2023. <https://www.dekk.institute/wp-content/uploads/2023/10/en-dekk-report-trendy-nedovery-2023-web.pdf>

²⁰ HAJDU et al. (2023)

²¹ Dušan FÁBIK: Prečo Slovensko podlieha ruskej propagande? DenníkN, 22 August 2023. <https://dennikn.sk/3532347/preco-slovensko-podlieha-ruskej-propagande/?ref=tit>

²² ŠTEPANOVIČ (2021)

²³ Standard media are locally informally defined as those that follow standard professional-ethical journalistic norms.

same time, almost 70% of followers of alternative media also follow standard media.²⁴ This data may help to explain why authorities decided to approach tackling online disinformation by banning some of these alternative media outlets, as we shall discuss further.

Therefore, probably all initial efforts and policies aimed at countering disinformation were based on false premises – ie. that popularity of disinformation is primarily the result of effective foreign (especially Russian) subversive propaganda. We shall see that such erroneous arguments and followup policies were often used to justify (or could be detected in background discussion and in normative justifications) regulatory – and other counter-measures. It is such measures that we will be discussing next.

First, we shall discuss the regulatory background. -Then, we shall discuss selected institutions and stakeholders who were involved in handling disinformation; we shall discuss their powers, obligations, tools and the procedures they used. Finally, a few negative examples of excessive scope in fighting misinformation shall be presented.

2. Regulatory overview

There are numerous strategic and conceptual documents (including draft-laws that were never adopted) produced by the authorities since 2018. There was temporary, severe and opaque regulation of local online news sources that were seen as ‘harmful’ to national security; this could actually be invoked ex officio by the National Security Authority (NSA or NBU) ex officio.²⁵ It is still not clear, or at least it has not been unambiguously interpreted by legal professionals, whether NSA can actually still block some websites (in addition to those related to cybersecurity incidents) upon the request of other parties. There is still hard-law regulation in place against some external (Russian) news sources following the invasion of Ukraine. This latter regulation followed pan-European *ad hoc* regulation.²⁶ We will discuss these issues later on.

Co-regulation of disinformation in online media – in particular social media – is by and large tackled at a supranational (European Union) level. However, there are some attempts which focus at regulating fake news and hoaxes in online media. We will discuss these later on, especially those that seem to be operating on longer and more professional basis.

There are quite a number of state institutions which tackle – or are supposed to tackle – disinformation in general, as a part of their activities. Some of them (e.g. the police) specialise (or rather specialised, following the change in governmental policies after the 2023 early general elections) in the fight against online disinformation in particular, as will be discussed further.

²⁴ Piško (2020)

²⁵ Local: Zoznam subjektov blokovaných EÚ. <https://www.nbu.gov.sk/zoznam-subjektov-blokovanych-eu/>

²⁶ EU: Council Decision (CFSP) 2022/2478 of 16 December 2022 amending Decision 2014/512/CFSP concernin <https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/19163-2/index.html> restrictive measures in view of Russia's actions destabilising the situation in Ukraine. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv%3AOJ.LI.2022.322.01.0614.01.ENG&toc=OJ%3AL%3A2022%3A322I%3ATOC>; Council Decision 2014/512/CFSP of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine [consolidated text]. <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02014D0512-20221204>

It should be noted that before the 2023 early general elections, state authorities (e.g. NSA), together with the European Commission and a US Senator, warned against possible online public disinformation campaigns, and put pressure on major platforms to prevent possible dissemination of the most problematic fake news and hoaxes (especially those based on AI – deep fake videos) (wire agency TASR [2023]²⁷, national security authority NBU [2023]²⁸). Indeed, such deepfake videos did appear towards the end of the electoral campaign (in particular, during the electoral blackout period).²⁹ One of these deepfake videos was critically reflected upon in post-elections period by Věra Jourová, the vice-chairperson of the Commission and the Commissioner for transparency and values.³⁰ From a legal regulatory point of view, deepfake videos highlighted a problematic enforcement of the blackout period.³¹ Interestingly, the police investigation concluded that “no sane person could ever believe its content”.³² In fact, this fake video was massively disseminated via Telegram, Facebook, TikTok, Instagram, YouTube, but also via WhatsApp, before the general election. Wider dissemination of this fake video was limited as a result of intervention of specialised governmental units entrusted with the fight against disinformation.³³ This case has not been closed at the time of writing – the prosecutor has re-opened the investigation into this case, and Reporters without Borders has even suggested that such messages should be criminalised.³⁴

Finally, it should be recalled that a new government lead by Robert Fico (since October 2023) has radically modified or strengthened the coordination of state policies towards disinformation, which we will be discussing in the next section. This included a new Concept of Strategic Communication of the Slovak Republic, approved by the Government in

²⁷ TASR: V USA žiadajú Metu, aby pred voľbami v SR nešírila ruské dezinformácie. *Teraz.sk*, 13 September 2023. <https://www.teraz.sk/spravy/americky-senator-vyzval-metu-aby-pred/740397-clanok.html>

²⁸ Varovanie v súvislosti s voľbami do NR SR 2023, <https://www.nbu.gov.sk/varovanie-v-suvislosti-s-volbami-do-nr-sr-2023/>

²⁹ Filip STRUHÁRIK: Šíria sa falošné nahrávky politikov. Nieкого môžu pobaviť, podstatné je, že majú ovplyvniť voľby. *DenníkN*, 29 September 2023. <https://dennikn.sk/3595174/siria-sa-falosne-nahravky-politikov-nieкого-mozu-pobavit-podstatne-je-ze-maju-ovplyvnit-volby/>

³⁰ Robert BARCA: Údajná nahrávka telefonátu predsedu PS a novinárky Denníka N vykazuje podľa expertov početné známky manipulácie. *AFP Slovensko*, 28 September 2023. <https://fakty.afp.com/doc.afp.com.33WY9LF>; Česká Tisková Kancelář: Slovenské volby provázela bezprecedentní dezinformační masáž, myslí si Jourová. *Aktuálně.cz*, 1 October 2023. <https://zpravy.aktualne.cz/zahranici/slovenske-volby-provazela-bezprecedentni-dezinformacni-masaz/r-59a28b50605f11eea25a0cc47ab5f122/>

³¹ See Martina HILBERTOVÁ – Michal PIŠKO – Ľuboš KOSTELANSKÝ: Moratórium dezinformácie nezastavilo, mohli tak ovplyvňovať voličov, *DenníkN Blog*, 7 December 2023. <https://dennikn.sk/blog/3625432/moratorium-dezinformacie-nezastavilo-mohli-tak-ovplyvnovat-volicov/>

³² Vladimír ŠNÍDL: Polícia odmietla vyšetrovať predvolebný deepfake. Nikto súdny mu vraj nemohol veriť. *DenníkN*, 14 January 2024. <https://dennikn.sk/3777044/policia-odmietla-vysetrovat-predvolebny-deepfake-nikto-sudny-mu-vraj-nemohol-verit/?ref=list>

³³ Vladimír ŠNÍDL: Podvrh rozhovoru predsedu ps pred voľbami ukázal, že deepfake slovenčinu nezvláda. onedlho to umelá inteligencia zvládne. *DenníkN*, 6 October 2023. <https://dennikn.sk/3608268/predvolebny-deepfake-nebol-kvalitny-proti-proruskym-kanalom-zakrocil-stat-coskoro-to-moze-byt-horsie/>

³⁴ RSF: As the investigation into a Slovak journalist Monika Tódová's 'deepfake' is reopened, RSF is calling for this type of attack to be criminalised. *RSF*, 6 March 2024. <https://rsf.org/en/investigation-slovak-journalist-monika-t%C3%B3dov%C3%A1-s-deepfake-reopened-rsf-calling-type-attack-be>, see also interview with journalist Tódová: #RSFTalks: Journalist Monika Tódová, victim of a deepfake to influence the election in Slovakia. *RSF YouTube*, 6 March 2024. https://m.youtube.com/watch?si=FJfhiGa4iqGjzXjc&fbclid=IwAR26CptfoRYSveKJpy3yHeBlhirsLz_u1tf0Hyp-k5QQGWaXeUqKsws1MjE&v=LXhX3Elvypo&feature=youtu.be

March 2024 (although the document itself is dated 2023). In this document, it was explicitly stated by the Government that the goal was to prevent a situation in which “NGOs would perform strategic communication of the State on their own, without accepting responsibility for the impact on Slovak society”.³⁵ Instead, the key role was taken over by the ‘Coordination Organ for Strategic Communication at the Office of the Government of Slovak Republic’.

2.1. State regulation

A temporary regulation on online disinformation was passed immediately after the Russian invasion of Ukraine, but this was short lived and was only in force during spring and summer of 2022.³⁶ As mentioned, there is legal ambiguity over whether the NSA can still block some websites with controversial content (with allegedly harmful content of political nature), at the request of other state authorities. The NSA provided only a general answer on that point, citing law, but not clearly answering this question when it was sent via e-mail.³⁷ (A pan-European ban on selected Russian media is still in force.) It should be noted that “taking action against media companies who broadcast infringing content has so far been the exclusive competence of Member States. War, as a special situation, has been exempted from this rule under the Regulation and under other exceptional circumstances.”³⁸

By contrast since 2023, the NSA has not been able to block online disinformation *ex officio*. As mentioned, this is in fact a contested issue. Some lawyers, e.g. Mesarčík³⁹ agree that although the NSA cannot block websites *ex officio*, specified third parties can actually ask the NSA to block websites. It should be clarified that there is no question of whether the NSA can fully or partially ban or limit usage of certain products (e.g. some online applications, processes, or services related to e.g. cybersecurity). We shall discuss this former controversial issue later on in section 2.1.2.

The Manifesto of the Government (2021–2024)⁴⁰ already included a plan to tackle dissemination of disinformation and hoaxes through criminal law.⁴¹ The plan was described as follows: “The Government of the Slovak Republic will examine the increase in the protection of interests of the Slovak Republic through criminal law standards against the risk of hybrids threats, especially related to the spread of propaganda and disinformation, support for extremists groupings and cyber attacks.”⁴² There is no legal definition of

³⁵ Koncepcia strategickej komunikácie Slovenskej republiky. UV SR (2024). https://www.hybridnehrozby.sk/wp-content/uploads/2023/08/koncepcia_strategickej-komunikacie_sr.pdf

³⁶ Then valid § 27b and § 27c Act 69/2018 on Cybersecurity.

³⁷ E-mail letter No. 04940/2024/SRD/ORM-002, dated 05.03.2024, signed by plk. Ing. JUDr. Alexandra Kaľavská Dianišková.

³⁸ KOLTAY (2023) 52.

³⁹ MESARČÍK (2023)

⁴⁰ As mentioned, there were early general elections in September 2023.

⁴¹ Programové vyhlásenie vlády Slovenskej republiky na obdobie rokov 2021–2024 (PVVSR 2021–2024). <https://www.nrsr.sk/web/Dynamic/DocumentPreview.aspx?DocID=494677>

⁴² Ibid., 11.

disinformation. Legal expert Mesarčík⁴³ believes that this lack of legal definition of disinformation is actually a good thing. In his view, “[i]t could happen that the definition would be too broad or too narrow and would not capture the cases we want to regulate”. In any case, previous temporary regulation, as well as various drafts usually did not use the term ‘disinformation’ specifically or exclusively, but, approached this issue inconsistently. For example, they used the terms ‘online threats’ or ‘hybrid threats’ or ‘harmful content’ or used other linguistic terms as described further on in this paper. However, it should be noted that the Constitutional Court (III. ÚS 288/2017/112) has found that there is a difference between ‘disinformation’ versus ‘untruth’. The Constitutional Court has also differentiated between ‘disinformation’ versus ‘information for the purpose/targeted information’ (účelové informácie) (PL. ÚS 26/2019).⁴⁴

The Manifesto of the Government reflected “concern of the Government with the increase of disinformation in the media and in particular on social networks, which is for the purpose of evoking fear and distrust in state and liberal democracy. Therefore, the Government [...] will support initiatives fighting hoaxes, fake news and other disinformation, as well as creating mechanisms to fight hoaxes, fake news and other disinformation.”⁴⁵ The Manifesto of the Government included many mentions which reflected concerns about disinformation as well as suggesting measures against disinformation, in various sectors of the government.

Indeed, there had been discussion about at least three drafts (including one submitted with substantial changes at a later stage) that were intended to regulate controversial online content, especially – in effect – on social media. However, neither of these proposals (draft laws) materialised during previous governments lead by Igor Matovič (2020–2021) or by Eduard Heger (2021–2023), or during the provisional government lead by Ľudovít Ódor (2023). We will discuss these draft proposals on regulation of disinformation later on in section 2.1.3. since these are interesting case studies. They both illustrate the efforts and arguments leading up to statutory regulation. As mentioned, the Cybersecurity Act (69/2018 Z.z., 2022 updated versions) actually regulated fake news and hoaxes under a temporary regulatory approach in 2022. This temporary legal regulation, which is probably no longer in force (at least not used since mid-2022) will also be discussed here. There was a plan to continue regulating disinformation further (including maintaining the option of banning some alternative media) but the Parliament did not approve a draft proposal to that effect of the Cabinet in 2022 (UV-42058/2022).⁴⁶ Among the suggested changes was that the Supreme Administrative Court should be involved as guarantor of legality, and NSA should publish all decisions on its website. The current version [§ 27b sec (7)] includes the right to appeal to a court. It also mentions that this appeal (to the administrative court) has no immediate/postponing effect on the decision in question. However, no blocking order have been issued by the NSA since March 2022.

⁴³ Veci verejné: Prepis diskusie Pozrime sa na to na TA3: Môžeme hovoriť a písať čo chceme? aj s Romanom Michelkom. Veci verejné, 22 November 2023. <https://web.archive.org/web/20231122145154/https://veci-verejne.sk/prepis-diskusie-pozrime-sa-na-to-na-ta3-mozeme-hovorit-a-pisat-co-chceme-aj-s-romanom-michelkom/>

⁴⁴ MESARČÍK (2023): 30

⁴⁵ PVVSR 2021–2024: 130.

⁴⁶ Návrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov – nové znenie, UV-42058/2022, 26.10.2022. <https://rokovania.gov.sk/RVL/Material/27764/1>

Not well known within Slovakia and therefore also worth discussing here is a regulation of specific content in the Press Act (Act on Publications), passed after the Russian invasion of Ukraine (and mentioned with reference in footnote 6 above). This is actually transposition of pan-EU blocking legislation into domestic legislation.

2.1.1. Temporary regulation of fake news and hoaxes

The National Security Authority (NSA or NBU) was able to block either ‘harmful content’ or ‘harmful activity’ throughout half of the 2022 and (still may) fully or partially ban or limit usage of certain products (e.g. some online applications, processes, or services, due to cybersecurity concerns) (Act 69/2018 Z.z., updated versions). Following the Russian invasion of Ukraine, emergency regulation was swiftly passed [including Act 55/2022 Z.z. on Certain Measures Concerning Situation in Ukraine, as an update to Act 69/2018 Z.z., § 5, sec (1) letter *ag*), and in particular § 27b, § 27c] that allowed blocking of certain websites for a few months. In particular, blocking was targeted at [Act 69/2018 Z.z., § 27b, sec (3)] malicious/harmful content or malicious/harmful activity.

“Malicious content means a program resource or data that causes or may cause a cyber security incident. Malicious activity means any activity that causes or may cause a cyber security incident, fraudulent activity, theft of personal or sensitive data, serious misinformation and other forms of hybrid threats.”

However, due to heavy criticism originating among some lawyers, the opposition and NGOs, this regulation did not continue in force beyond September 30, 2022 [Act 231/2022 Z.z., an update to Act 69/2018 Z.z., § 27b, sec (9)].

The NSA was able to decide whether to block “harmful/malicious content or harmful/malicious activity that can cause serious disinformation or other forms of hybrid threats” [§ 27b sec (3)]. However, neither ‘disinformation’, nor ‘other forms of hybrid threats’ were defined in § 3 – ‘Clarification of Key Terms’. Interestingly, the NSA published an informal ‘Short Dictionary of Hybrid Threats’ on its web.⁴⁷ This online dictionary defines and explains ‘disinformation’ as well as ‘hybrid threats’.

The NSA was able to execute such decisions or block certain websites, following a request by a third person [§ 27c sec (1)], [further specified as a public authority, in effect meaning state authority, see also § 27b sec (8)], or ex officio decision [§ 27b sec (1)]. Interestingly, this activity could be carried out not only in cooperation with state authorities [§ 27b sec (8)], but also in cooperation with natural and legal persons – e.g. internet service providers [§ 27b sec (5), (6)]. The NSA should decide about blocking (according to the law) in such a way that blocking would be effective, expedient, and adequate to possible risks related to blocking [§ 27b sec (4)]. As mentioned, NSA was also able to decide about blocking ex officio, initially up until June 30; this was later extended until September 30, 2022 (Act 231/2022, an update to Act 69/2018 Z.z.). This regulation was de iure based on emergency Act 55/2022 (passed on February 26, 2022, just two days after the invasion began), which allowed and specified in article III, resulting in changes to Act 69/2018 Z.z. (arguably

⁴⁷ Krátky slovník hybridných hrozieb, <https://www.nbu.gov.sk/kratky-slovník-hybridnych-hrozieb/>

unconstitutional activity, as will be discussed later on) the blocking of certain websites by the NSA, initially effective until June 30, 2022.

The decision to block had to include [§ 27b sec (2)] identification of the authority, identification of the person running the infrastructure to be used for blocking, identification of harmful content or harmful activity, the reason for blocking, the method of blocking, terms for execution of blocking, duration of blocking, and options for ‘de-blocking’; finally, the decision had to include legal-administrative instructions (such as the possibility for appeal, if relevant). This should have prevented arbitrariness on the part of the NSA. If a third legal person were to ask the NSA for blocking [§ 27c sec (1)] of a certain subject, the administrative procedure conditions would be almost identical, and it would be specified that “the reason for blocking which should be an executable decision of requested authority” were to be included [§ 27c sec (2) letter *e*].

Similarly, costs associated with blocking – if such blocking was requested by a third person – were split. While damage caused by *execution* of blocking were charged to the NSA, costs associated with the act of blocking as well as *the cost of any damage caused by blocking* were charged to the applicant [§ 27c sec (7)]. This suggests that immediate and much lower costs were to be covered by the NSA, while long-term costs of such decision were to be covered – if such long-term costs arose – by the applicant.

The measure of blocking ‘harmful content’ passed in the spring and then extended in the summer of 2022 appears to no longer be in force (except those blockings related to ‘cybersecurity incidents’). However, as mentioned, this is legally controversial or at least a confusing issue. In § 27b, sec (9), it is stated that “Making decision on blocking of harmful content or harmful activity is possible only until 30 September 2022”. In § 27c sec (1) it is stated that “The NSA may also carry out blocking on the request of a subject according to a special document”. In a footnote, examples of these ‘special documents’ are given – the Act 46/1993 Z.z. on Slovak Intelligence Services and the Act 30/2019 Z.z. on gambling. This later Act 30/2019 Z.z. on gambling refers to Act 30/2019 Z.z. on electronic communications that [§ 41, sec (6)] stipulates that “an enterprise is obliged to limit access to website whose address is mentioned in court order”. However, this type of website blocking is carried out under the auspices of the Gambling Regulation Authority.

For execution of blocking based on the Act on cybersecurity [§ 27c sec (9)] “instructions of § 27b sec. (5)–(7) will be used appropriately”. In turn, these instructions are mostly of a technical nature. However, § 27b sec (7) also states that the decision to block is subject to appeal before the court, and administrative lawsuit do not have a delaying effect (nemá odkladný účinok). Thus, on the one hand, the NSA *may block at the request of another subject*. On the other hand, it *can not decide* about blocking. Ultimately, it is § 27b sec (2) which clearly sets out the formal requirements for issuing a blocking decision. Yet this § 27b sec (2) is in contradiction with § 27b sec (9), since the latter does not allow the NSA to act at all. So does this mean that the NSA may – in accordance with § 27c sec (1) – perform blocking without actually issuing a decision on a given case? This seems strange, but at the same time, § 27c sec (9) states explicitly that from among the provision of § 27b, only § 27b sec (5)–(7) are to be applied for performing blocking.

In any event, there has been a rather fierce discussion about the legality and constitutionality of these measures, as we shall discuss later on.⁴⁸ It should be noted that § 27a still allows “placing limits on the use of products, processes of services of a third party”. This is different level of regulation (in contrast to ‘blocking’ as mentioned in § 27b and in § 27c). There is also a justification for ‘banning or limiting’ when something “threatens the security interests of the Slovak Republic” [§ 27a, sec (1), letter *b*)]. In effect, theoretically, the NSA can still ban or limit certain use e.g. the use of news applications.

2.1.2. Regulatory efforts that did not materialise (draft legislation)

In addition to temporary regulation directly implemented by the NSA as discussed above (Act 55/2022 Z.z. as part of the Act on Cybersecurity) and actual blocking of selected news and current affairs websites, there were regulatory efforts that never made it into law. Due to space limitations, we shall not discuss *ad hoc* legal regulatory initiatives by MPs here, such as an initiative by deputies from OĽANO, SaS and Za ľudí parties in April 2021.⁴⁹

The first publicly available governmental draft text (an update to the Criminal Code) aimed at regulating fake news and hoaxes was a draft proposal prepared by the Ministry of Justice under Mária Kolíková (*Za ľudí – For the People Party*). It was a part of wider updates in criminal legislation. The draft was first submitted for public discussion in late 2021, and again (in a new version) in 2022. The draft proposal was justified primarily by COVID-19 pandemic controversies about the safety and efficiency of vaccination. However, this seemed to be just the reaction to the culmination of a longer trend of spreading conspiracy theories, fake news and hoaxes which had started some time earlier.

The specific section of the proposal (§ 361, part of larger update to Criminal Code) was called ‘The offence of Spreading Untrue Information’. Specifically, this crime was supposed to include “production and dissemination of knowingly untruthful information which is capable of causing a risk of serious concern/alarm (*znepokojenia*) at least among part of the population in a certain place, threatening the life or health of inhabitants or influencing inhabitants in their decision-making on serious issues of societal importance (ceľospoločenského významu)”. The suggested maximum criminality for such a crime was up to 10 years imprisonment. For example, even repeated cases of negligence dissemination of such ‘untrue information’ should be punishable up to a year imprisonment.

It should be noted that the Criminal Code (Act 300/2005 Z.z.) already includes ‘the offence of fearmongering’ (§ 361). The text of this paragraph is as follows: “Whoever willfully causes a risk of serious disturbance to at least part of the population of any place by spreading an alarming report which is false, or who commits other similar conduct

⁴⁸ It should be mentioned that at least one these previously blocked websites changed its territorial internet-based domicile as to avoid or complicate further attempts at blocking.

⁴⁹ For example, TASR: Koaliční poslanci chcú predĺžiť zákaz webov, ktoré považujú za dezinformačné. *Pravda*, 8. April 2022. <https://spravy.pravda.sk/domace/clanok/622943-koalici-poslanci-chcu-predlzit-zakaz-webov-ktore-povazuju-za-dezinformacne/>; Ivana ŠALGOVÁ: Boj štátu s hybridnými hrozbami Nevypíname neviniatka, ale štváčov, vraví Krúpa. Weby bude možné blokovať trvalo. *Postoj*, 25 April 2022. <https://www.postoj.sk/104458/nevypiname-neviniatka-ale-stvacov-vravi-krupa-blokovanie-webov-moze-byt-trvale>

capable of causing such a risk shall be punished by imprisonment of up to two years.” Depending on further conditions, the criminality may be of up to eight years imprisonment. Moreover, § 362 that states “Whoever, in a crisis situation of the state, causes a serious risk, even through negligence, anxiety, small-mindedness or defeatist mood in at least part of the population of some place, by spreading an alarming message, shall be punished by imprisonment from six months to three years.” Thus, this is even more strict regulation, as it is sufficient to be negligent in this case.

In any event, a draft proposal intended to introduce the ‘offence of spreading untrue information’ was criticised by many lawyers, NGOS as well as by both special and general prosecutors. For example, Maroš Žilinka, prosecutor general, called this draft “absurd, ambiguous and empirically impossibility to prove”. Therefore, it was seen as inappropriate proposal according to legal standards, as well as an inadequate regulatory reaction to the current situation in a society.⁵⁰

The second draft proposal with the strange working title ‘Act About Measures to Prevent Spreading Not-Allowed Content’ was aimed at “measures to prevent dissemination of unallowed content”.⁵¹ It was submitted for public discussion (PI/2022/83) by Veronika Remišová (Za ľudí – For the People Party), the then vice-prime minister and minister of investments, regional development and digitalisation in April 2022. The inspiration for ‘technical’ aspects of regulation was taken from Germany. The justification for such a proposal was found in two cases. In the first case, a student attacked fellow students with an axe. Moreover, in another hate crime, a student randomly killed LGBT+ persons, while expressing hatred also towards some local politicians and Jews. Both youngsters were supposed to have become radicalised on social media with conspiratorial content.⁵² However, a few months earlier justification for such a regulation was more standard – it included negative examples of disinformation which appeared during campaigns before the US elections in 2016, Brexit, the Russian annexation of Crimea, and campaigns by well-organised fascist movements, as well as allegedly many people who have been misled, including the most vulnerable groups, such as youngsters and seniors.⁵³ It appears that these regulatory efforts included previous consultations or initiatives at the EU level, as well as bilateral talks with representatives of Meta Company.⁵⁴

⁵⁰ TREND: The Criminal Act of Spreading False Information is Absurd and Inappropriate, Says Žilinka to Kolíková. *TREND*, 3 December 2023. <https://www.trend.sk/spravy/m-zilinka-novy-trestny-cin-sirenieneppravdivej-informacie-je-nenalezity>

⁵¹ Vicepremiérka Remišová: Nenávisť na sociálnych sieťach rozkladá demokratickú spoločnosť – nový zákon zavedie pravidlá pre platformy, ktoré takto zarábajú milióny eur. *MIRRI*, 20 April 2022. <https://mirri.gov.sk/aktuality/digitalna-agenda/vicepremierka-remisova-nenavist-na-socialnych-sietach-rozklada-demokraticku-spolocnost-novy-zakon-zavedie-pravidla-pre-platformy-ktore-takto-zarabaju-miliony-eur/>; PI/2022/83 Predbežná informácia k návrhu zákona o opatreniach proti šíreniu nedovoleného obsahu (012942/2022/OL-3), (PI/2022/83), 19.04.2022; <https://www.slov-lex.sk/legislativne-procesy/SK/PI/2022/83>

⁵² Branislav CABAN: Ministerka Remišová chce zákonom regulovať sociálne siete, rozdeľujú podľa nej spoločnosť. *Touchit*, 9 November 2022. <https://touchit.sk/remisova-chce-regulovat-socialne-siete/450791>

⁵³ Vicepremiérka Remišová na Globsecu 2022: Sociálne platformy musia prebrať väčšiu zodpovednosť za škodlivý obsah, ktorý šíria. *MIRRI*, 2 July 2021. <https://mirri.gov.sk/aktuality/podpredsednicka-vlady/vicepremierka-remisova-na-globsecu-2022-socialne-platformy-musia-prebrat-vacsiau-zodpovednost-za-skodlivy-obsah-ktory-siria/>

⁵⁴ Adriána Belej MAJERČINOVÁ: Remišová sa stretla s predstaviteľmi Facebooku. Rezort chystá právnu reguláciu mesiace. *Pravda*, 21 October 2022. <https://spravy.pravda.sk/domace/clanok/644463-remisova-sa-stretla-s-predstavitelmi-facebooku-nas-rezort-chysta-pravnu-regulaciu-digitalnych-platforiem/>

With regard to the type of content which was intended to be regulated by this draft law, there was a rather broad focus. It was supposed to have included almost all existing criminal offences such as sexual abuse, blackmail, making threats, (electronic) harassment, spreading alarming news, defamation of nation, race, and belief or incitement to national, race, or ethnic hatred, treason, collaboration with enemy or espionage. Thus, this was supposed to be *lex generalis*. It was planned to be used when there was a case of spreading forbidden content via electronic services used for sharing content with other users. The draft law focused on ‘services’ with higher number of users. The responsible entity was supposed to be a service provider and it was the service provider who was supposed to check controversial content, once it was reported to them. If the content was found to be against the rules, the service provider was supposed to prevent further dissemination.

In case of violation of this obligation, the state would have been able to impose monetary sanctions on service operators, impose the obligation to remove illegal content and, in extreme cases, even block the service provider nationwide, as it has already done, for example, with the disinformation portal *Hlavné správy* (translated as Headlines or Main News).

The regulation was intended to introduce an obligation for electronic service providers to allow users to verify their identity and mark their profiles as official, as is the case today, e.g. on social networks (previously Twitter, now X, or Instagram). Such profiles should be clearly marked as verified, so that it was clear that it was not a fake profile impersonating another person or company.

For the purposes of preparing the draft law, the Ministry also suggested a definition of the terms ‘disinformation’ and ‘hoax’.

“The law should distinguish between them according to the following definitions: disinformation:

1. demonstrably (or obviously) false, misleading or manipulatively presented information that is intentionally created, presented and disseminated with the clear aim of lying or misleading, capable of causing some harm or securing some benefit;
2. often contains an element that is obviously true, which gives it credibility and can thus complicate its detection;
3. misinformation does not include inadvertent errors in reporting (factual error), satire and parodies, or biased reports and comments that are clearly marked as such;

hoax:

1. a virally spread fake news or deliberate lie;
2. usually has three typical features – (i) urgency, (ii) reference to an illusory authority and (iii) request for further dissemination;
3. often the intention is to induce alarm or fear.”⁵⁵

These definitions were criticised during the public legislative process as “having included elements which are obviously true, which give it credibility and can thus complicate its detection; misinformation”. Such a definition of disinformation can be applied to any manipula-

⁵⁵ Stanislav VINC: Štát chce regulovať sociálne siete. Ak nezmažú hoax, môže ich pokutovať. *Techbox*, 20 April 2022. <https://www.techbox.sk/stat-chce-regulovat-socialne-siete-sirenje-hoaxov-by-mal-pokutovat>

tive information which could lead to confusion in terminology, argued the Office of the Government and Chancellery of the Security Council.⁵⁶ Furthermore,

“at the same time, the need to define the term ‘hoax’ is redundant, as it basically meets the definition of disinformation (‘deliberate lying’). Also, the typical features of a hoax mentioned in the text (‘urgency, reference to illusory authority, request to spread’) are features applicable to the concept of disinformation.”⁵⁷

The Office of the Prosecutor General demanded, as a ‘fundamental request’, to delete the words

“dissemination of untruthful information according to § 361a and 362”. In contrast, the Ministry of Foreign and European Affairs suggested adding “in addition to the term information operations also to use a term disinformation, alternatively (also include) disinformation activity (pôsobenie) or deliberate dissemination of untruthful and misleading information.”

Additional criticism of the draft law included its redundancy in view of existing measure or measures that were at that time in process of introduction, such as more active communication by state authorities towards citizens. The Slovak Chamber of Attorneys argued that § 361 of the Criminal Code already covers such crime (dissemination of untruthful information). The Ministry of Culture as well as (then) Broadcasting and Retransmission Board (now Media Services Board) pointed out that there was already a draft law on Media Services (transposed EU Directive 2010/13/EU) undergoing a second reading in the Parliament. The draft law on media services introduced proceedings to prevent the spread of illegal content on a content-sharing platform (in particular, § 112, § 151, § 152 and § 153). Moreover, the Ministry of Culture argued that it had exclusive competence to regulate content in general. The Ministry of Interior (Hybrid Threats Centre) suggested to re-consider the use of the term ‘illegal content’ itself, as it falls exclusively under the jurisdiction of the courts to assess whether the elements of the criminal offense are fulfilled, as well as to take a decision on guilt and punishment. Finally, it was also seen as essential to re-assess whether the proposed legislation limits the constitutional right to freedom of speech and the free dissemination of information.

The third proposal was submitted for public and professional discussion in March 2023, under the working title ‘LP/2023/129 Act on Measures to Increase Security and Trustworthiness of Platforms in Online Environments’. The author of this draft proposal was once again the Ministry for Investments, Regional Development and Information lead by Veronika Remišová. There were 184 comments raised in the public legislative process.⁵⁸

⁵⁶ Predbežná informácia k návrhu zákona o opatreniach proti šíreniu nedovoleného obsahu. *Slov-Lex*, 2022. https://www.slov-lex.sk/legislativne-procesy?p_p_lifecycle=0&p_p_col_id=column-2&_processDetail_WAR_portletset_action=pplpZobrazPripomienky&p_p_id=processDetail_WAR_portletset&_processDetail_WAR_portletset_cisloLP=PI%2F2022%2F83&p_p_col_count=1

⁵⁷ Ibid.

⁵⁸ LP/2023/129, Zákon o opatreniach na zvýšenie bezpečnosti a dôveryhodnosti platforiem v on-line prostredí a o zmene a doplnení niektorých zákonov. <https://www.slov-lex.sk/legislativne-procesy/SK/LP/2023/129/pripomienky/zobraz?page=2>

The draft included a definition of disinformation (§ 2) as “unambiguously untruthful information, created, presented and disseminated with the aim of deceiving society (klamať verejnosť) or a certain group of persons, the consequence of which is or may be damage, or detriment or contribute to benefit (zabezpečenie prospechu)”.

Clearly, there were many formal and specific objections against these draft laws, so let us return to broader and currently valid regulatory options.

2.1.3. Currently valid legal regulations on fake news and hoaxes

There is no specific local hard law regulation tackling fake news and hoaxes directly or generally in the online environment in Slovakia. However, there have always been legal regulations that tackle what are broadly understood as being fake news and hoaxes, either online or offline. These legal tools include public personal or institutional libel (civil or criminal law), or defamation of race, nation, or religion (criminal law), or publishing ‘a false or incomplete factual claim’ (the press law and the Act on Media Services), or broadcasting ‘illegal content’ (formerly audiovisual regulation, now the Act on Media Services) to name a few typical examples.

However following the Russian invasion of Ukraine, the Act on Publications (‘the Press Law’) includes a specific ban on the dissemination of certain information, as defined by state authorities or supranational bodies (the EU). This recent regulation should also of interest to us. It covers specifically online versions of offline publishing activities. In effect, it introduces, or transfers supranational censorship into the national domain. Let us first discuss a more general law which covers video-sharing platforms.

The Act on Media Services (264/2022 Z.z.)

This act applies to a broadcaster of a radio programme service, retransmission services and multiplex providers, if they have a registered office or place of business or residence in Slovakia. There are more detailed conditions for television broadcasters and (§ 7) video-sharing platforms (including § 9 ‘content-sharing platforms’, if there is the aim to make profit, e.g. works protected by the Copyright Act). The regulator (MSB) is also entitled (§ 110) to assess the appropriateness of measures taken by video sharing platform provider to protect the public.

A 2024 update (Act passed on 27 June 2024, without numbering) gives regulatory rights over content sharing platforms as well as engine search providers [§ 108 sec (1)] to the MSB.⁵⁹ Moreover, § 108 sec (6) specifies that central state authorities and public administration in general have to cooperate with the MSB. The MSB is referred to as the ‘coordinator of digital services’, which includes audiovisual services on demand, content sharing platforms and internet search engines – in addition to those legal subjects mentioned earlier. In

⁵⁹ Zákon z 27. júna 2024, ktorým sa mení a dopĺňa zákon č. 264/2022 Z. z. o mediálnych službách a o zmene a doplnení niektorých zákonov (zákon o mediálnych službách) v znení neskorších predpisov a o zmene a doplnení niektorých zákonov, https://www.slov-lex.sk/ezbierky/pravne-predpisy/SK/ZZ/2024/203/vyhlasene_znenie.html.

[§ 109 sec (2)], it is stipulated that the regulator performs supervision of whether legal documents that tackle content sharing platforms are followed. Perhaps redundantly, this is further highlighted in § 109 sec (3), letter *c*), where state regulation of content sharing platforms is mentioned. However, both these legal rights and duties of the MSB [§ 109 sec (2) and § 109 sec (3), letter *c*)] have only been in force since 28 June 2025. Finally [§ 110 sec (3), letters *w*)–*y*)] entrust the MSB to fulfill the tasks of coordinator of digital services, to participate at work in European Committee for Digital Services, and, among other tasks, to entrust, temporarily postpone or remove status of trustworthy reporter (understood as concerning problematic content online).

The Act on Media Services is obviously of more general purpose than just regulating fake news or hoaxes. Yet it should be noted that even before 2024 (2025 respectively) there was a regulatory sea-change §110 sec (3) letter *q*), which allows cooperation with platforms with respect to their content moderation practices and in an effort to enforce their respective ‘community’ standards. This cooperation should aim at the efficient, proportional and non-discriminatory application of services’ standards. In fact, until 2024 or 2025 respectively, the MSB could only take action if potentially illegal content was being spread online. These cases of problematic content include child pornography, extremist materials, posts inciting terrorism or national, racial and ethnic hatred, posts denying or approving the Holocaust and crimes against humanity, or posts defaming a nation, race or belief. Obviously, some may argue that, for example, some extremist material is at the same time disinformation (or fake news and hoaxes). In such case, however, the argument should be made (if one turns to this legislation with respect to tackling disinformation) that it is – for example – in the first instance, output which is ‘extremist’ or ‘defaming a nation, race or belief’. Before users turn to the regulatory authority with a request for intervention, the operators of the website on which the illegal content is being spread must be notified (§ 152). This is relevant where potentially illegal content is found on a content-sharing platform, or in particular for electronic periodic publications, news webportal, or wire agency portal [§ 152 (2)].

Whether the content breaches the law will be decided by the board’s three-member panels. If the Board comes to the conclusion that the content in question is illegal and at the same time its dissemination threatens the public interest or represents a significant interference with individual rights citizens, it will issue a decision to prevent its spread. If the platform operators do not remove the illegal content and do not prevent it from spreading further, they may be fined between 2,500 and 100,000 euro by the Board.

During the period 1 August 2022 – 10 November 2023, the Media Services Board dealt with 53 cases of possible online illegal content. However, only in 2 cases were official legal-administrative procedures initiated. The first case concerned a blog post published on the *hlavnespravdy.sk* portal, which questioned the number of victims of the Holocaust and at the same time contained hateful comments interwoven with conspiracy theories about members of the Jewish ethnicity and their role on a global scale (AO-RPMS/2022/00254). The second case (AO-RPMS/2023/00143) tackled comments under a video posted by a municipality on the YouTube video sharing platform to news channels. The video concerned the exclusion of members of the Roma ethnic group from a public transport vehicle. A comment containing hate speech appeared under this video, calling for the extermination of this ethnic minority.

However, as could have been expected, disinformation cases did not fall under the competences of the Media Services Board. For example, in the case AO-RPMS/2023/01084, the Board dismissed the case (presenting pro-Russian propaganda on social network) due to a lack of any illegal component. The possibility that disinformation was included was insufficient.⁶⁰

As previously mentioned, some forms of fake news and hoaxes have been dealt in general terms in § 212. “If a false or incomplete statement of fact was mentioned in the broadcast program, which affects the honor, dignity or privacy of a natural person or the good reputation of a legal entity, on the basis of which the person can be precisely determined, this person has the right to reply (strictly linguistically, in Slovakia it is called ‘the right to expression’).”

The Press Act (The Act on Publications 265/2022 Z.z.)

This act (officially it is called the Act on Publications) regulates the obligations of the publisher of a periodical publication, the operator of a news web portal and a news agency when disseminating information, and obligations of the publisher of a non-periodical publication when distributing publications. It also tackles self-regulatory mechanisms. As mentioned, § 8 defines the Right to Expression. Specifically,

“If a false or incomplete factual claim has been mentioned in a periodical publication or agency service which interferes with the honour, dignity or privacy of a natural person or with the reputation of a legal person, on the basis of which the person can be accurately identified, that person has the right to have the statement published. The publisher of a periodical publication, the operator of a news web portal and a news agency are obliged to publish a statement at the request of this person.”

Furthermore, there is § 9 and the Right to Supplementary Notice:

“If a periodical publication or agency service containing communiqués of a journalistic nature or communiqués of a journalistic nature contains a factual claim of proceedings before a public authority against a person on the basis of which the person can be precisely identified, and this proceeding has been terminated by a final decision, that person shall have the right to request the publication of a supplementary notice of the final outcome of those proceedings.”

Interestingly, a new § 4 section 2 defines that:

“The publisher of a periodical, the operator of a news web portal and a news agency are obliged to ensure that they do not allow the end user or the public access to content the provision of which is prohibited to persons, entities, bodies or their representatives or intermediaries under a special regulation directly or through a periodical publication published or made available to the public.”

⁶⁰ MESARČÍK (2023): 112–117.

In a footnote, this content is defined as “for example, Articles 2f and 12 of Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia’s actions destabilising the situation in Ukraine (OJ L 229, 31.7.2014), as amended.” In other words, there is an obligation for censorship of certain types of information as requested by the state authorities or by supranational authorities. There are sanctions, too, in case of breach – notification of a violation of the law or a fine of up to € 20,000. One might wonder whether this is in line with the Constitution that ‘forbids censorship’ (Article 26, sentence 3). It is true that the next sentence (4) of the Constitution allows for exceptions to ban on censorship: “Freedom of speech and the right to seek and disseminate information can be limited by law if the measures in a democratic society are necessary to protect the rights and freedoms of others, the security of the state, public order, and the protection of public health and morals.” Moreover, it is stated in Article 13 (2) of the Constitution that: “The limits of fundamental rights and freedoms can be adjusted under the conditions established by this Constitution only by law.” Thus, although this censorship was established by the law, does it really fulfill all other conditions as defined in Article 26(3) of the Constitution? Slovakia was not at war with Russia, and it is highly questionable whether a few Russian disinformation webportals can be seen as a threat to “the security of the state, public order, and the protection of public health and morals.” Unlike in the case of right to expression, or right to additional announcement, the purpose of this institute is not the protection of the personal rights of individual persons (or good reputation of a legal entity), but rather the protection of the public interest. From a constitutional perspective, in each case it must be determined which particular ‘public interest’ is to be protected and if measures taken are appropriate. At a first glance, one may argue that this provision does not impose any new restrictions on publishers or news agencies, as this is already given by the applicable legislation defining or determining ‘prohibited content’.

The Cybersecurity Act (Act 69/2018 Z.z.)

As mentioned, the Cybersecurity Act is the only act which has tackled fake news and hoaxes explicitly and relatively systematically in Slovakia – albeit for a temporary period in 2022 – but it did so in what was arguably an unconstitutional manner. Currently, cooperation and providing information “important for securing cybersecurity and solving cybersecurity incident” for fulfilling tasks due to a cybersecurity event is still compulsory for public authorities, as well as for providers of ‘basic services’ and ‘legal entities’ as defined in Appendix 1 of the Act on Cybersecurity. There is a caveat: it is only obligatory to provide such information which is ‘necessary’ for resolving the cybersecurity incident. However, Appendix 1 lists not only essential ‘digital services infrastructure’ but practically all industrial sectors (such as transport, energy sector, etc).

Furthermore, as previously mentioned, the NSA can ban or limit the use of certain products (e.g. some applications), processes, or services, if it finds that they do not enable, or in a fundamentally hamper cybersecurity (§ 27a). It can be assumed that this ban may include social media applications. For this regulation to apply, there must be a risk to life and health of persons, the economy of the state, public order, or property .

Furthermore, these potential threats to cybersecurity include “the security interests of Slovakia”. In such situation, the NSA (§ 27a) can act *ex officio*, or following a request from another public authority (here the term used is ‘public’, not ‘state’). Information on initiating such regulatory initiative must be published at least 30 days prior totaking action, in a single information system for cybersecurity, as well as on the NSA website. Interestingly, during this ‘waiting’ period the NSA can not issue a decision. Any decision has to be preceded by analysis of risks (in cooperation with the Ministry of Foreign Affairs, Ministry of Economy, Ministry of Interior, Slovak Intelligence Services, and Ministry of Defense. A draft proposal is then submitted to the Security Council and the Government [Cabinet of Ministers]). The opinion of the Government is binding for making any decision.

There is another condition – the decision of the NSA is conditioned by activity or lack of thereof of the third party in question. In other words, the decision will be issued only if a provider of basic services or a third party, do not make the requested corrections within a reasonable deadline as set by the NSA. Finally, if there is a decision by the NSA, this must be published in the Collection of Laws. There is time limitation for such total or partial ban. The NSA has to stipulate a reasonable period for banning or limiting usage of certain product, process, or service. This period cannot be longer than for two years. However, it is possible to issue such a full or partial ban repeatedly. There are also sanctions – these are between 300 euro up to 1% of overall turnover, with a maximum in value of 300,000 euro.

With respect to blocking controversial content, it is instructive to mention that the NSA just a year earlier (i.e. in 2021) explicitly stated that it does not have a legal right to collect content of communications. Moreover, the NSA stated that all blocking has to follow administrative law procedures. The NSA argued that it regularly informs the Special Supervising Committee of the Parliament in annual reports, as well as providing any other requested information. The NSA argued that all its decisions are subject to review by the Constitutional Court. Finally, blocking on the request of another legal subject was originally requested by the Ministry of Economy. It was meant to be a supplementary tool in cases concerning consumer protection – with reference to a European regulation. Blocking on request from a third party was accepted by other state authorities such as the Ministry of Defense, Ministry of Interior and Consumer Protection Authority.⁶¹

2.2. Conceptual regulatory documents

The authorities have enacted mostly cross-sectoral documents which partly or entirely tackle disinformation (as, for example, one of the identified it as ‘hybrid threats’). However, it should be mentioned that some of them are no longer valid:

⁶¹ NBÚ: Reakcia NBÚ na medializované informácie k novele zákona o kybernetickej bezpečnosti. *NBÚ*, 31 March 2021. <https://www.nbu.gov.sk/reakcia-nbu-na-medializovane-informacie-k-novele-zakona-o-kybernetickej-bezpecnosti/>

*2.2.1. The Concept of the Slovak Republic's fight against hybrid threats (2018)*⁶²

This concise (six pages) conceptual document summarised an emerging institutional framework for tackling the issue of hybrids threats. The main purpose of the document was to set up a mechanism for information exchange and evaluation. It also defined basic indicators for hybrid threats, of which online disinformation was merely one of many. The document stated that on the one hand, not a single department possesses material, technical and human resources for full coverage of this issue. On the other hand, it argued, hybrid threats demonstrate cross-sectoral and inter-institutional features. The document summarised the role of the two most important overarching (coordinating) bodies: the national contact point for hybrid threats – Situational Center (SITCEN) – and the national cooperation centre for hybrid threats, the National Security and Analytical Centre (NBAC). Which institution actually drew up this document and when is not clearly stated.

2.2.2. The Manifesto of the Government (2020–2024) (PVVSR 2021–2024)

The most important task in this field was “to prepare an action plan to coordinate the fight against hybrid threats and the spread of disinformation and build adequate central capacities for its implementation”. As previously mentioned, the Government announced its aims to “examine the increase in the protection of interests of the Slovak Republic through criminal law standards against the risk of hybrids threats, especially related to the spread of propaganda and disinformation, support for extremists groupings and cyber attacks”. Furthermore, the Manifesto stated that the Government “will support initiatives aiming at fighting hoaxes, fake news and other disinformation”. The Ministry of Defense was asked “to take into account the changing security environment in the context of cyber and hybrid threats, misinformation, climate change and challenges resulting from technological development, including AI”. There was also a plan to update the content of education and training towards critical thinking, with the aim of creating better resistance to conspiracy theories and misinformation.

*2.2.3. The Action plan for coordinating the fight against hybrid threats for the period from 2022 to 2024 (NBU [2022])*⁶³

This 22 page document was drawn up by the Ministry of Defence. It includes the following sections: General tasks, Systematic measures, Strategic communication and disinformation, Building the resilience of society, Protection of electoral processes and Foreign influence. The Action Plan represents a reaction to “the security risks associated with foreign investments in critical infrastructure, media, or the academic sector, influencing election process-

⁶² Konceptcia pre boj Slovenskej republiky proti hybridným hrozbám. NBÚ, 2018. <https://www.nbu.gov.sk/data/att/1126.pdf>

⁶³ <https://www.nbu.gov.sk/akcny-plan-koordinacie-boja-proti-hybridnym-hrozbam/>

es, strategic corruption, or the action of disloyal paramilitary groups, with increased emphasis on subversive influence activities of actors, using propaganda and disinformation or spreading hate speech or extremist content”.

2.2.4. *Security Strategy 2021*

This strategy is the key strategic document for state security. It explicitly names the readiness to effectively respond to hybrid threats as one of its strategic interests and contains a commitment to increase Slovakia’s resilience.⁶⁴ Specifically, it defines among its ‘strategic security interests’ resistance of the state and society to security threats as well as citizens’ trust in a democratic state and independent public institutions and social cohesion. This is in response to “the increase in importance and scope of non-military threats and procedures”. The Security Strategy highlights that

“The number and scope of subversive and coercive activities by various actors is increasing using disinformation and propaganda to disable or manipulate decision-making mechanisms in the state, to influence public opinion in their favor and destabilise the political situation... The public is exposed to the increasing spread of misinformation and conspiracy theories that can threaten human health, subvert cohesion society or provoke public violence and social unrest.”

2.3. Self and co-regulation of online disinformation

In the light of the lack of an overarching effective hard law regulation for disinformation in online environment, a grass-root process has developed some attempts to create self or co-regulation. However, the overview of the annual reports of the main or potentially the most important self-regulatory body – the Press and Digital Board of the Slovak Republic (TRSR) – suggests that it has not yet got involved in any activity that would tackle disinformation in online news and current affairs webportals. This may be partly explained by the very essence of self-regulation, in as much as that very much depends on the good will of those involved. In addition, self-regulation of digital (and print) media in Slovakia can be seen as having a confusing design. Although according to Section I, subsection 1, letter *a*) of the Code of Journalistic Ethics, this Code is binding “for natural persons and legal entities that issue periodical or non-periodical print in print or digital version intended for distribution in the Slovak Republic”, at the same time, those natural persons and legal entities have to first publicly declare their willingness to follow this Code of Ethics.⁶⁵ In contrast, and paradoxically, the scope of the Statute of TRSR encompasses virtually all natural persons and legal entities active in this field (without mentioning their prior declaration of willingness to be covered by this self-regulation).⁶⁶

⁶⁴ Bezpečnostná stratégia Slovenskej republiky. *MOSR*, 2021. https://www.mosr.sk/data/files/4263_210128-bezpecnostna-strategia-sr-2021.pdf

⁶⁵ Etický kódex novinára. https://www.aonesr.sk/wp-content/uploads/2025/06/Etický_kodex.pdf

⁶⁶ Štatút tlačovo-digitálnej rady Slovenskej republiky. https://web.archive.org/web/20240629122646/http://trsr.sk/wp-content/uploads/2016/05/Statut_TR_SR-1.pdf

The Code of Ethics of Electronic Media addresses advertising and marketing communication only. It has been in effect since 2010.⁶⁷ Similarly, the Code of Use of Content from the Internet deals only with copyright-related issues.⁶⁸ It should be noted that there is a new self-regulatory initiative: the Ethical Code for Marketing Influencers.⁶⁹ This Ethical Code has been drafted by the Interactive Advertising Bureau Slovakia (IAB Slovakia) and Association of Digital Marketing Agencies (ADMA) in 2022. Potentially, it can be assumed that influencers may disseminate fake news and hoaxes. However, no such case has as yet been identified. Therefore, this initiative shall not be discussed in any further detail here.

By virtue of its nature, the co-regulatory body, the Advertising Council, can only tackle online disinformation on an ad hoc basis, if at all.

Then there remains enforced self-regulation, as represented by the webportal and associated NGO Konšpiratori.sk. This involves trying to indirectly impose some moral and monetary pressure on controversial online news and current affairs portals, as well as many other dubious online resources. Konšpiratori.sk is one of many NGOs and private initiatives involved in enforced regulation or simply in monitoring disinformation in the online environment. Next, we shall discuss only those which were operating in 2022. For example, an anti-hoax initiative by online versions of the quality liberal newspaper *Sme* (hoax.sme.sk), which ended its activities in 2021.

2.3.1. Webportal Konšpiratori.sk (*Conspirators*)

This webportal is a cross-border or two-nation (covering both Czech Republic and Slovakia) attempt to disclose the monetary income from ads in online advertising flowing towards controversial quasi-journalistic online sources, which are seen by some actors as being involved in production and dissemination of fake news and hoaxes; it is operated by an NGO. This is an approach which involves disclosing online disinformation indirectly. The webportal (NGO) provides a list of ‘controversial’ websites and more recently (since September 2023), ‘controversial’ YouTube channels, or, those of a ‘conspiratorial’ nature, as the original name (translated as ‘conspirators’) suggests. In other words, it provides a list of those involved in ‘conspiratory’ style reporting and commenting online. Specifically, it claims that it is “a public database of websites with non-serious, deceptive, fraudulent, conspiratorial or propaganda content”.⁷⁰ Next, the initiative specifies that “we compile a list of websites and YouTube channels where members of our committee have doubts about their credibility and quality of content”.⁷¹ The list includes approximately 300 items. These are categorised from one to 10 (worst). There is also ‘a grey zone’. This grey zone includes websites with an index in the range of 6–4. These domains (about 30) currently allegedly do not

⁶⁷ IABSlovakia: Etický kódex elektronických médií, *IABSlovakia*, 2009. <https://www.iabslovakia.sk/wp-content/uploads/2023/04/IABsk-Etický-kodex-elektronických-médií.pdf>

⁶⁸ IABSlovakia: Kódex preberania obsahu na internete, *IABSlovakia*, 2022. https://www.iabslovakia.sk/wp-content/uploads/2023/02/KODEX_preberania_obsahu_24_06_2022.pdf

⁶⁹ The Ethical Code for Marketing Influencers. <https://kodexinfluencermarketingu.sk>

⁷⁰ <https://konspiratori.sk/>

⁷¹ <https://konspiratori.sk/zoznam-stranok>

represent a significant risk for brands, but the Evaluation (expert) Commission is still paying attention to their activities, it continuously observes and reevaluates the content on these webdomains.

Four interesting legal case studies emerged as a result of this initiative. Two of them involved major controversial news and current affairs webportals (*Hlavný denník* and *Hlavnespravy.sk*) and two of these webportals (*Parlamentnilisty.cz* and *AC24*) were actually originally from the Czech Republic.⁷² All four websites sued the initiative based on business law court cases or injunctions. This was in itself an unusual, and initially quite effective self-defense. The final verdicts have been handed down, except in the case of *Parlamentnilisty.cz*. Thus, for *Parlamentnilisty.cz*, there is (at the time of writing) an ‘urgent injunction’ in place. Activity regarding further court proceedings has been slow.

Hlavný denník request that the court issue an “urgent injunction against the NGO for unfair interference into its business activities”. More specifically, it claimed that being included on the list of controversial sources may cause a negative and immediate business impact and could be seen as unfair business practice – in effect, giving advantage to its competitors. Therefore, it asked the court to order an ‘urgent injunction’ that would prohibit including *Hlavný denník* on the list. Lower courts accepted this request. However, *Hlavný denník* did not proceed further with the regular court case for two years, so the Supreme Court considered that this ‘urgent injunction’ had lasted too long. Moreover, the Supreme Court did not see any unfair business practice in issuing such a ‘recommendation’ by the NGO.⁷³ There were no further legal steps taken from the side of *Hlavný denník*.

In a similar case, *Hlavnespravy.sk*, was again placed on the list of controversial websites, after years (2018–2022) of court battles. Interestingly, the court considered the decision and assessment of the National Security Authority (NBU) in its judgement. The NBU argued that this online outlet represents a ‘security threat’.⁷⁴

The court case initiated by the Czech webportal *AC24* attempted to follow identical legal argumentation as it was used in previous cases (business law – urgent injunction). However, in this case both county and regional court in Slovakia dismissed this motion in 2022.

It should be mentioned that the first verdict in which webportal *Hlavnespravy.sk* used the argument of ‘reputation damage’ by Konšpirátori.sk NGO was handed down in October 2023. The lower court dismissed the case as unfounded.⁷⁵ because it accepted monitor-

⁷² Konšpirátori.sk: Konšpirátorom dočasne stiahnúť web hlavnespravy.sk zo svojej databázy. *DenníkN Blog*, 3 March 2020. <https://dennikn.sk/blog/1775813/sud-prikazal-konspiratorom-docasne-stiahnut-web-hlavnespravy-sk-zo-svojej-databazy/>; P Konšpirátori.sk: arlamentnilisty.cz sa súdia s Konšpirátormi. Je to ako žalovať Google za zlé recenzie, odkazujú im autori projektu. *DenníkN Blog*, 4 December 2020. <https://dennikn.sk/blog/2170626/parlamentnilisty-cz-sa-sudia-s-konspiratormi-je-to-ako-zalovat-google-za-zle-recenzie-odkazuju-im-autori-projektu/>; Konšpirátori.sk: Web, ktorý straší peklom a tvrdí, že očkovanie zabíja, musí ísť dole zo zoznamu Konšpirátorov. *DenníkN Blog*, 12 August 2021. <https://dennikn.sk/blog/2501424/web-ktory-strasi-peklom-a-tvrdi-ze-ockovanie-zabija-musi-ist-dole-zo-zoznamu-konspiratorov/>

⁷³ Konšpirátori.sk: Hlavný denník neuspel ani na Najvyššom súde, putuje späť na zoznam dezinfowebov. *DenníkN Blog*, 19 May 2022. <https://dennikn.sk/blog/3378382/hlavny-dennik-neuspel-ani-na-najvyssom-sude-putuje-spat-na-zoznam-dezinfowebov/>

⁷⁴ Konšpirátori.sk: Hlavné správy putujú späť na zoznam dezinfowebov. *DenníkN Blog*, 22 December 2023. <https://dennikn.sk/blog/3161411/hlavne-spravy-putuju-spat-na-zoznam-dezinfowebov/>

⁷⁵ Konšpirátori.sk: Hlavné správy prehrali súd s projektom Konšpirátori.sk. *DenníkN Blog*, 30 October 2023. <https://dennikn.sk/blog/3652929/hlavne-spravy-prehrali-sud-s-projektom-konspiratori-sk/>

ing activity as lying within the limits of freedom of expression. However, the court also used a less important argument: the fact that the NBU had also blocked the website, so there were reasons for monitoring this webportal.⁷⁶ Interestingly, the verdict about the constitutionality and legality of blocking by the NBU (which is part of a separate court case) has not yet been issued. There is an interesting legal analysis of this case study written before the court's verdict.⁷⁷

2.3.2. *The Advertising Council*

The Advertising Council has existed for a much longer time. However, the Advertising Council only signed up to the self-regulatory mechanism in October 2023. This is in line with § 130 of the Act on Media Services which set up a co-regulatory alternative in advertising regulation. This development is potentially relevant here, there are two major TV networks among members of the Advertising Council: the Association of Radio Stations of Slovakia and the oldest news TV TA3, and public media RTVS (now STVR). They all have their own websites, and in most cases presence on social media such as Facebook. Yet it remains questionable whether and how the Advertising Council will become involved in regulating online disinformation effectively, if at all.

2.3.3. *The Press and Digital Board of the Slovak Republic*

In the print sector (including online print) there is the Press and Digital Board of the Slovak Republic (TRSR, in old terms, the Press Council). AONE, the Association for Protection of Journalistic Ethics (the founding body of the Press and Digital Board) has incorporated among its members the Interactive Advertising Bureau Slovakia (IAB Slovakia) in 2017. Since then, the Press and Digital Board, as defined in the founding charter of AONE, seeks: “to supervise the maintenance of ethical principles of journalistic work in print and digital media created in Slovakia (...)”.⁷⁸ The scope of its mission is also specified in § 2 of the Statute of the Press and Digital Board as including among its legitimate targets: “natural and legal persons who run websites (webpages) on which there are published products of journalistic activities of natural persons or editorial offices of periodical and non-periodical press, intended for dissemination in the Slovak Republic”.⁷⁹

The Press and Digital Board discussed ethical issues that appeared in online versions of (primarily) offline publications in three of all six cases which were submitted to it, exclu-

⁷⁶ 30.10.2023, Dnes sudkyňa na prvostupňovom súde rozhodla v náš neprospech v spore s Konšpirátormi, <https://www.hlavnespravy.sk/dnes-sudkyňa-na-prvostupnovom-súde-rozhodla-v-nas-neprospech-v-spore-s-konspiratormi/3304090>

⁷⁷ LANGER (2023)

⁷⁸ Asociácia na Ochranu Novinárskej Etiky: Stanovy Asociácie na ochranu novinárskej etiky v Slovenskej republike. AONE, https://www.aonesr.sk/wp-content/uploads/2016/05/Stanovy_AONE_09.2021.pdf

⁷⁹ Štatút tlačovo-digitálnej rady Slovenskej republiky. https://web.archive.org/web/20240629122646/http://trsr.sk/wp-content/uploads/2016/05/Statut_TR_SR-1.pdf

sively or partially, in 2022.⁸⁰ In 2021, the number of online-only ethical cases reached about the same number – four out of nine cases (of which two were originally submitted in 2020).⁸¹ Finally, in 2020, it was possible to identify four out of 10 cases (three from 2019) as originating exclusively from online publishing activity.⁸² However, none of the above online cases dealt with typical fake news or hoaxes. They merely involved biased, incorrect or unfair reporting.

3. Institutions/stakeholders involved in tackling disinformation: issues, powers, obligations, tools and procedures

In general, it is likely easier to mention authorities and institutions which are *not* involved in handling disinformation in Slovakia.

3.1. State authorities

The list of institutional members of the Committee for Hybrid Threats of the Security Council of Slovakia defines all key state actors that are seen as relevant stakeholders in this field. These are *a)* Ministry of Foreign Affairs and European Affairs, *b)* Ministry of Defense, *c)* Ministry of the Interior, *d)* Ministry of Economy, *e)* Ministry of Finance, *f)* Ministry of Investments, Regional Development and Information, *g)* Ministry of Transport, *h)* Ministry of Health, *i)* Ministry of Justice, *j)* Ministry of Culture, *k)* Ministry of Education, Science, Research and Sports, *l)* Ministry of Labour, Social Affairs and Family, *m)* Office of the Government, *n)* the Authority of Nuclear Supervision, *o)* National Security Authority, *p)* Slovak Intelligence Service, including additional representative of Department for security threats, *r)* Military intelligence, and finally *s)* the Police. Since 2024, the Office of the Government has been the key coordinating body here, as we shall explain later on.

In general, state authorities must, according to the Action Plan (AP), put “emphasis on cooperation with alliances (ie NATO) partners, centers of excellence, etc. when performing tasks through entrusted state organs”. Furthermore, there has to be an “emphasis on cooperation with the academic sector, i.e. domestic as well as foreign universities, research organisations and professional public in the performance of tasks through entrusted state organs”.

⁸⁰ Výročná správa 2022. https://web.archive.org/web/20240719053756/https://trsr.sk/wp-content/uploads/2016/05/TR_SR_VS_2022.pdf

⁸¹ Výročná správa 2021. https://web.archive.org/web/20240712144058/http://trsr.sk/wp-content/uploads/2016/05/TR_SR_VS_2021.pdf

⁸² Výročná správa 2020. https://web.archive.org/web/20221006045334/https://trsr.sk/wp-content/uploads/2016/05/TR_SR_VS_2020.pdf

Among specific tasks, there was a plan to include strategic communication under the organisational statutes of all ministries and the Office of the Government, by a deadline of the first quarter of 2023.⁸³

Furthermore, state authorities are obliged, as stated in the Concept of the Slovak Republic's fight against hybrid threats, to initially evaluate the reported hybrid threats incidents falling under their competence, and according to the definitions of indicators set out in the Concept of the Slovak Republic's fight against hybrid threats, they then have to forward information about an incident meeting any of the hybrid threat indicators) for further processing, assessment or evaluation by the National Security Analytical Center (NBAC). State authorities also have to provide information additionally to the reported information, which will be evaluated by the NBAC to decide whether it is a hybrid threat. When doing so, state authorities shall follow their own internal regulations or legal regulations for security incidents.

In addition to generally mentioned and specifically defined state authorities, we present selected state authorities which have been specifically designated to tackle disinformation. The following order of appearance of selected institutions does not represent any subordination or indicate the level of importance of those institutions: in fact, the relationships between them are quite complex and intertwined.

3.1.1. The National Security Authority (NSA or NBU) and in particular, its National Security Analytical Center (NBAC)

The NBAC is the national cooperation center for hybrid threats. Its main functions are to collect information where there is a suspicion of a hybrid threat and classify under the evaluation process by creating an NBAC file. After a statement from the state authorities represented in NBAC, in cooperation with SITCEN, it should add 'context' to the relevant NBAC file from the point of view of EU and NATO security interests and further decide whether there is a need to process the output for the recipients.

3.1.2. Center Against Hybrid Threats (CBHH)

The Ministry of Interior (MV) has established a Center Against Hybrid Threats (CBHH) within the Slovakian Police. The task of the CBHH is to increase the resilience of society through activities such as monitoring and processing analytical outputs, especially in relation to the MV. With regard to 'Hoaxes and Scams', the Facebook page of the Police claims to be the most followed page in Slovakia which focusses on misinformation, with almost 150,000 followers in 2023. It has been online since 2018. The selection criteria for hoaxes and frauds (many of which are suggested by Facebook users) are: mass sharing on Facebook (or potential for such mass impact), topic seemed to be interesting and have a clear message addressed to the national public. One of the most common disinformation narratives that it

⁸³ Akčný plán koordinácie boja proti hybridným hrozbám 2022–2024. NBU, 2022. <https://www.nbu.gov.sk/data/att/1127.pdf>

debunked was related to foreign affairs: the pandemic is a secret plan by the powerful to rule over or destroy humanity. Significantly, the 2021 Report raised the issue of foreign actor involvement: “It is possible that their actions were trying to support the foreign policy interests of state powers abroad. Foreign state powers tried to spread their narratives through their own media or allied media, or via fictitious independent activists, often communicating in different ways within their own state.”⁸⁴ The Police is also present on Instagram. However, these debunking activities are very controversial and often slip into subjective statements and comments, which are beyond the statutory competence of the Police. Since late 2023, there has been change in focus of the CBHH.

3.1.3. The Ministry of Justice

The Ministry of Justice drafted the first governmental draft aimed at regulating fake news and hoaxes *in 2021*.

3.1.4. The Ministry of Defence

As mentioned above, the Ministry of Defence has been involved in drafting some strategic documents. In addition, it was assigned to produce an “In-depth vulnerability analysis of selected bodies of the state administration against hybrid threats”, with a deadline of December 2022 (AP). It has established the Department for Hybrid Threats and Strategic Communication in 2022. The main activities of the department include the creation of a situation overview, analysis of the impact of information operations and implementation of reactive and preventive measures intended for mitigating their consequences.⁸⁵ The Ministry of Defence produced analytical material focused on the income of ‘controversial’ websites from commercial activities (ads).⁸⁶

3.1.5. The Ministry of Foreign Affairs and European Integration

The Ministry of Foreign Affairs and European Integration is responsible for efficiency, ability to act as well development of tools and initiatives of NATO, the EU and other organisations in the fight against hybrids threats (Action Plan – AP). Moreover, it was the first state ministerial body which established a special unit for this agenda, in the form of the Department for Strengthening Resilience and Hybrid Threats in May 2020.

⁸⁴ See *Police Force Report on Disinformation of the Slovak Republic in 2021*. Communication and Prevention Department of the Presidium of the Police Force, 2022. 5. https://www.minv.sk/swift_data/source/images/slovak-republic-report-dezinfo-2021.pdf

⁸⁵ 2022 Ročenka Ministerstva Obrany SR. MOSR, 2022. https://www.mosr.sk/data/files/5032_rocenka_2022_print.pdf

⁸⁶ ŠTEPANOVIČ (2021)

3.1.6. The Security Council

The Security Council is a permanent advisory, initiative and coordination body of the Government in the area of state security. The key task of the Security Council is to participate in the creation and implementation of a reliable security system for Slovakia, and to ensure the coordination of measures on the practical implementation of tasks in the field of security and the state's international obligations. The Security Council is expected to prepare proposals for maintaining the security of the state and to prevent crisis situations (including proposals for solutions to such crisis situations). For example, it is tasked with producing an annual report on the fulfillment of the Action plan for coordinating the fight against hybrid threats from 2022–2024. Day to day work is performed by the Office of the Security Council. The Office ensures the fulfillment of coordination, professional and consultative tasks in the field of security for Slovakia.⁸⁷

3.1.7. The Committee for Hybrid Threats of the Security Council of Slovakia

The Committee for Hybrid Threats of the Security Council of Slovakia (as one of the permanent committees of the Security Council) was established in 2023 (Act 97/2023 Z.z. as supplement to the Act 110/2004). The main mission of the Committee for Hybrid Threats is to coordinate activities intended to evaluate the security situation at home and abroad, while taking measures to deal with hybrid action against the interests of the country, and drafting relevant policies in the field of combating hybrid threats. The law defines the tasks of the Committee quite extensively. The Committee for Hybrid Threats is tasked to report on the results of the evaluation to the Office of the Security Council, at least once a year. On behalf of the Security Council, it has to draw up proposals for measures to increase the resistance of the state and society to the risks of hybrid action. It participates in shaping policy and drafting conceptual documents in the field of hybrid threats, as well as in the coordination of interdepartmental and international cooperation in the field of hybrid threats. It also has to make proposals to the Security Council for measures to increase society-wide awareness of hybrid threats. It is expected to discuss proposals submitted to the Security Council, which are related to the performance of tasks in the field of hybrid threats. Finally, it has to prepare expert analyses related to hybrid threats and submit them to the Security Council, and assess drafts of binding legal regulations and international treaties related to hybrid threats, which are submitted for discussion by the Security Council.

3.1.8. The Situational Center of the Slovak Republic (SITCEN)

The Situational Center of the Slovak Republic (SITCEN) is no longer defined as the national contact point for hybrid threats, but since 2024, it has been defined as a “government information analytical workplace with nationwide scope for the field of evaluating changes in

⁸⁷ Štatút Bezpečnostnej rady Slovenskej republiky. https://www.vlada.gov.sk/site/assets/files/1765/s_tatu_t_u_lohy_kbr.pdf

the security environment”⁸⁸ – SITCEN’s roles are therefore wider than previously defined. Hybrid threats are just one of seven broadly defined threats.

3.1.9. The Office of the Government

The Office of the Government is also active in this field. For example, the Department for Strategic Communication of the Government Office of the Slovak Republic and the Slovak Debating Association jointly launched a project to support the development of critical thinking and digital literacy for students from five randomly selected secondary schools in various regions of Slovakia in 2023. The topics included digital citizenship, misinformation and hybrid threats. as mentioned earlier, since 2024, SITCON has been in existence with a new mission under the Chancellory of the Security Council. However, employees are paid by the Office of the Government. Similarly, as mentioned, a new Statute of the Office of the Government [Art. 5, letter *m*)] specifies that the Office oversees the activities of the Chancellory of the Security Council. Most importantly, according to the Concept of Strategic Communication of the Slovak Republic, the Office of the Government has been the key coordinating body at a national level since early 2024.⁸⁹

3.2. Non-governmental and private entities

There is a surprising variety of non-governmental and private entities involved in the fight against disinformation. This selection is perhaps representative of this diversity of funding, focus, scope, approaches used and intensity, as well as the timescale for their involvement.

3.2.1. AFP⁹⁰

Since 2020, the national agency TASR has been cooperating with AFP’s (Agence France-Press) fact-checking programme (since 2023 there are two fact-checkers). The French agency provides this programme in cooperation with Facebook (Meta) and other relevant partners. The project produces photographs with descriptions, online status, videos and other evidence documenting when a hoax is identified. Once a post is rated

⁸⁸ Štatút Situačného centra Slovenskej republiky. https://www.vlada.gov.sk/site/assets/files/1765/statut_situacneho_centra_slovenskej_republiky.pdf

⁸⁹ Konceptia strategickkej komunikácie Slovenskej republiky. https://www.hybridnehrozby.sk/wp-content/uploads/2023/08/konceptia_strategickej-komunikacie_sr.pdf

⁹⁰ See Martin HODÁŠ: Overuje správy pre Facebook. Hoax vymyslíte za 10 minút. Vyvraciame ho celé dni [It verifies messages for Facebook. You can make up a hoax in 10 minutes. We spend days refuting it.]. *ZIVE*, 9 May 2020. <https://zive.aktuality.sk/clanok/146760/overuje-spravy-pre-facebook-hoax-vymyslite-za-10-minut-vyvraciame-ho-cele-dni/>

as ‘false’ by a fact-checker, it will appear lower in the News Feed and be displayed with a warning on Facebook.⁹¹

3.2.2. ‘Elfs’

‘Elfs’ or Elfovia.sk (elv.ai) is a start-up focused on monitoring of online comments. It is based on human and machine (AI) monitoring and intervention. The project employs a team of people tasked to remove misinformation, hate speech and block trolls from social media discussions. It cooperates (offers such services) for over 100 websites (for both Czech Republic and Slovakia), mostly media outlets such as private *TV Markíza* and private *Radio Express*. However, moderation also covers some public institutions and non-governmental organisations, including, for example, the Representation of the European Commission. Content moderation takes place in their own software (previously used Zoomsphere), which allows the semi-automatic processing of all comments on the profiles of the media websites concerned. Elf only relies on posts of a few sources (initially it was just a single medium). About 20 percent of online comments require being hidden or deleted. During one or maximum two hours shifts (initially it was a four-hour shift), an elf manages to go through 1,400 to 1,700 posts. In total, about 40,000 comments can be checked daily.

3.2.3. Demagog

Demagog.sk and *Demagog.cz* are fact-checking portals. They primarily check the statements of politicians and other publicly active persons which are made in political discussions or in the public sphere. However, occasionally, they focus on fake news and hoaxes.⁹² In particular, *Demagog.cz* in cooperation with Meta (Facebook) has focused on fake news and hoaxes in Slovakia.⁹³ Since 2010, *Demagog.sk* has analysed more than 700 political debates and more than 15,000 factual statements.

3.2.4. Infosecurity.sk

The information and watchdog platform *Infosecurity.sk* publishes a biweekly report on emerging disinformation trends. The portal also produces a regular podcast series, Disinfo report, which is published on a weekly basis and is unique in that it is the only podcast series focused on disinformation and other forms of non-factual content. The project also strives to raise public awareness and build social resilience by publishing web content (authored articles), a regular weekly newsletter on disinformation, preparing fact-checks in co-

⁹¹ Check permanently updated list of identified fake news and hoaxes at: <https://fakty.afp.com/list>

⁹² See Pavol VALÍK: Umelo vytvorený hlas Michala Šimečku vyzýva na zdrazenie piva. *Demagog.sk*, 27 September 2023. <https://demagog.sk/umelo-vytvoreny-hlas-michala-simecku-vyzyva-na-zdrazenie-piva>

⁹³ See <https://demagog.cz/tag/slovensko>

operation with CEDMO, or publishing reports and research studies with different thematic focus within projects with domestic and foreign partners.

3.2.5. Hoax.sk

Webportal *Hoax.sk* was founded in 2012. It publishes a few examples of hoaxes/fake news annually. In addition, it documents internet scams such identity theft. The project is run by volunteers and it is unique in that it has been operating without any subsidies for over a decade.

3.2.6. Seesame

PR company Seesame created what it claims is the first Facebook chatbot ‘Checkbot’ to help detect fake news on the web. It is based on verification of a link to the article in Facebook chat. Checkbot should recognise the words most commonly used by fake news media and disinformation sites. It is also capable of performing a reverse image search of images used in the article and will report on how many manipulations it found. It is claimed that there were more than 6,000 users, including 50 media companies of this chatbot’s services. Facebook chat users with Checkbot can be warned when a hoax is being spread on the Internet and the bot can be managed by a live admin team as needed. It should be noted that Seesame was behind a fictitious public conflict between two local YouTubers based on a false report in 2017. On the sixth day, a joint video was released where they explained that the purpose of this campaign was to highlight the problem of misinformation and fake news. It was a part of a video series that was targeting 500,000 12–18 years olds.

3.2.7. Globsec

Globsec is a global think-tank with local office in Bratislava. It has a Centre for Democracy & Resilience which conducts research in the field of information operations and hybrid threats. In December 2022, this Centre for Democracy & Resilience became a part of the European Digital Media Observatory (EDMO), which specialises in the fight against disinformation. In addition, Globsec became a participant in the VIGILANT project in late 2022. That project was intended to equip Police Authorities and individual officers with disinformation identification and analysis tools, technology, and knowledge that would make their fight against criminal online content easier and more effective.

3.2.9. CEDMO

The Central European Center for Digital Media Observatory (CEDMO) is a project – a multidisciplinary hub funded by the European Commission. It aims to identify, research and prioritise the most critical sources and causes of information issues in Slovakia (also in Czechia and Poland).

3.2.10. *KInIT*

KInIT is an independent, non-profit institute dedicated to intelligent technology research. The members of KInIT have produced some studies on fake news and disinformation.⁹⁴

3.2.11. *Blbec.online*

Blbec.online is another online project which does not receive any funding. Volunteers create a list of Facebook pages and profiles (over 1,800), for which the contributors have doubts about their trustworthiness and the quality of content. Moreover, it provides the ability to manage one's own discussions on Facebook. There is a unique function such as Autopilot, which automatically hides comments from unwanted people. Another function allows users to set up individualised Facebook monitoring.

Additionally, there have been many ad hoc (short-term) campaigns, studies or projects. For example, there were campaigns run by O2 telephone operator (2021), MEMO98.sk NGO (2022) and hackathon Hacknime.to (2022). A comparative overview report suggested as policy recommendations that the key issue is to increase media literacy and critical thinking.⁹⁵ Therefore, the weakest link among institutions was identified as being the Ministry of Education. In addition, continuous cooperation between non-governmental and governmental sectors was highlighted as very beneficial to all parties.

4. Practice

In this section, we discuss five interesting case studies which reflect the legal-constitutional, political-diplomatic and methodological challenges when in fighting disinformation, as well as the challenges faced by activists.

4.1. Case study: Constitutional challenges with the ban on 'alternative' news and current affairs portals in early 2022

The temporary ban on selected 'alternative' online news and current affairs portals was widely seen as unconstitutional. It should be explained that all these webportals have been placed on the list of 'controversial' websites by konspiratori.sk NGO. On the one hand it is true that these were not typical news and current affairs portals but rather hastily produced collection of usually unverified claims and gossip. On the other hand, it was also true that these webportals tended to publish stories that have often been ignored by the major traditional media (online or offline). This blocking was widely seen as controversial from a legal point of view; specifically because the justification given was too vague and it was in breach of ECtHR case law — *OOO Flavus and others against Russia*. This intervention was taken

⁹⁴ SIMKO et al. (2022); HRCKOVA et al. (2022).

⁹⁵ PISKLOVÁ–SÝKORA (2021)

by the NSA and justified on the vague grounds of “blocking harmful activity”. More specifically, it was stated that the NSA “has identified harmful activity that may produce serious disinformation”. No further specific evidence or arguments were mentioned or made available. These were classified as ‘sensitive’ (dôverné) and ‘secret’. The law did not define ‘serious disinformation’. The director of the NSA further justified the blocking and its scope, arguing that “blocking should be effective, with purpose and able to address possible risks associated with blocking”. Legal experts criticise this measure.⁹⁶

4.2. Case study: Globsec and its methodological problem with the ‘Vulnerability index’

It is argued here that the Vulnerability Index, which was developed as an analytical tool, is misleading. The Vulnerability Index (2021) analyzed the ‘vulnerabilities’ of selected countries to foreign malign influence in five dimensions: public attitudes, political landscape, public administration, information landscape and civic and academic space. There is also a Kremlin Influence Index produced by another international team.

On a scale of 1–100 (0 is the most resilient and 100 the most vulnerable) the Vulnerability Index for 2021 evaluated vulnerability to Russian and Chinese influence in Czechia (at 29 points), Slovakia (at 32) and Hungary (at 44), while data for Poland were unavailable. An earlier Vulnerability Index (2017) identified Hungary (at 57 points) as the most vulnerable country, closely followed by Slovakia (51), then followed at some distance by both Czechia (38) and Poland (30).

Similarly, based on a different methodology, the Kremlin Influence Index (2017) produced the following scores: Hungary 61, Czechia 48, Georgia 54, and Ukraine 49, identifying Hungary as the country most vulnerable to Russian influence over processes in the information space, ie. the production, exchange and consumption of information.

In contrast to the basic assumptions behind the Vulnerability Index and the Kremlin Influence Index, in both cases one sees more of a self-induced vulnerability or congruence of chosen foreign policies with selected foreign actors, rather than the impact of some foreign propaganda/public diplomacy or misinformation and disinformation. This differing analytical perspective is not just a minor challenge to either index. Rather, it has fundamental analytical, and in effect, policy consequences. In that sense, it is also instructive for searching for the proper approach to fighting or tackling disinformation. In short, among analysts there is analytical confusion or an unacknowledged convergence between ‘vulnerability’ and ‘congruence’. Congruence suggests a more active approach and in effect, a policy choice. It also suggests the limited impact of propaganda (or fake news and disinformation). In con-

⁹⁶ Peter ŠAMKO: Blokovanie webových stránok a jeho možný rozpor s judikatúrou Európskeho súdu pre ľudské práva. *Právne listy*, 26 February 2022. <http://www.pravnelisty.sk/clanky/a1062-blokovanie-webovych-stranok-a-jeho-mozny-rozpor-s-judikaturou-europskeho-sudu-pre-ludske-prava>; Martin HUSOVEC: Súčasné blokovanie dezinformačných stránok je ústavne problematické. Čo s tým? [The Current Blocking of Disinformation Sites is Constitutionally Problematic. What About That?] *DenníkN*, 22 April 2022. <https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/>

trast, vulnerability paints rather passive actors – possibly because of the huge impact on propaganda and limited foreign policy choices.⁹⁷

4.3. Case study: Educational activism which turns into disseminating disinformation

An NGO, MEMO'98 and Globsec produced two short brochures with the aim to educate people in general, and elderly people in particular about disinformation. The first booklet is called 'War in Ukraine and energy. Questions and answers'. This brochure aims to "raise awareness of the energy crisis and its solutions" and was published by Globsec. The second booklet was published under the title 'Seniors in the light of information'. This brochure was "intended as a basis for conversations on the topic (...) within the framework of discussions with seniors", and was published as part of the project Increasing the resistance of Central European seniors to misinformation by MEMO'98.

A fundamental problem with the text of the first booklet (War in Ukraine and energy. Questions and Answers) is that it claims

"Russia has long used the supply of its mineral resources, especially oil and gas, to exert geopolitical pressure on various countries. Such activities include artificially raising the prices of oil and gas, reducing supplies or completely shutting off the flow of these raw materials, or building new gas pipelines that bypass transit countries of the former Soviet Union with which Moscow had disagreements" (p. 12).

In fact, this basic statement is not true. In the long run, i.e. for decades, Russia (the former Soviet Union) has fulfilled its oil and gas supply obligations. Finally, if Russia were to proceed in a long-term and systematic way in the case of supplies of such raw materials (oil and gas), transported mainly by oil and gas pipelines, as described in the brochure, no one (or only a gambler) would extend existing long-term agreements with it, or conclude new trade agreements. No new gas or oil pipelines would ever be built. Russia would have to pay repeatedly large sanctions for violating trade agreements. Nothing like this is known. Such a procedure could not even be in the interest of Russia, which would needlessly spend huge sums on unnecessary, producing loss making rather than profit making gas and oil pipelines. The examples given by the brochure (two-day and 12-day supply interruptions through some gas pipelines, and further unspecified 'interrupted supplies' over the last 20 years), basically do not confirm, but refute the basic thesis of the brochure (p. 12).

The second booklet is aimed at seniors. What will seniors learn? Among other things, two or three controversial, or partially or completely false statements:

- a) Questioning (by the authors of the publication) the statement that: "Measures to restrict movement and other anti-pandemic measures are a threat to democracy and human rights" (p. 16). In fact, the Constitutional Court declared some measures

⁹⁷ Andrej ŠKOLKAY: Vulnerable 'Vulnerability Index' – or what we got wrong with analysis of Hungary's foreign and domestic policies. *DenníkN Blog*, 13 April 2023. <https://dennikn.sk/blog/3324338/vulnerable-vulnerability-index-or-what-we-got-wrong-with-analysis-of-hungarys-foreign-and-domestic-policies/>

- restricting movement during the pandemic to be unconstitutional – parts of the law on the protection of public health, especially those related to mandatory state quarantine elsewhere than in the home environment. Since the decision of the ÚS SR zn. PL. ÚS 4/2021 was issued in 2021, and the cited publication was issued in 2022, it is not true that these claims about a threat to democracy and human rights are “dubious claims” and that “all of them can be unequivocally refuted by facts” (p.16).
- b) Questioning (by the authors of the publication) the statement that: “Kyiv bans the Russian language and culture”. (p. 17). If we were writing this before 2019, the authors of the publication would be more or less right. In 2023, it was only partially true. The Russian language was not banned in common usage but Russian culture certainly was.
 - c) Questioning (by the authors of the publication) the statement that: “The Russian army only attacks military targets, never civilians” (p. 17). This statement is, of course, true as it is formulated. But no army can absolutely rule what is called collateral damage during the war. Moreover, some objects have, or can have, both a civilian and a military character (e.g. energy infrastructure or airports).

4.4. State authorities and dissemination of fake news online

The Slovak Embassy in France claimed on Facebook in August 2022 that it was Russia that had attacked Georgia in 2008. Following the same reasoning, the Slovak Ambassador in the UK claimed on Facebook that it was Russia that attacked Georgia in 2008.⁹⁸ In fact, although the official position of the Ministry of Foreign Affairs and European Integration of Slovakia was identical,⁹⁹ an Independent International Fact-Finding Mission on the Conflict in Georgia found out that it was Georgia that initiated that conflict.¹⁰⁰ There are many cited studies that – sometimes reluctantly – accept that this time Russia was not an aggressor, or at least not the side which fired first.

4.5. NGO Konšpirátori.sk and controversial assessment of online news webportal *Standard.sk*

As it was discussed in section 2.3.1, self-regulatory activities in the civil society has raised some interesting legal case studies. However, there is a particularly controversial case study within this civil society activism that may or may not end in court, but nonetheless deserves a mention here. In summary, one (*Standard.sk*)¹⁰¹ of two relatively recently (2020, 2015) es-

⁹⁸ Exact wording of public statement by Igor Slobodník, ambassador of Slovakia to France, was: “That one anniversary is 7 August 2008, when Georgia was attacked by neighbouring Russia” (8 August 2022). Robert Ondrejcsák, ambassador to the UK, wrote similar statement the same day on Facebook: “Open aggression of Russia against its neighbours started already in 2008, by attack on Georgia.”

⁹⁹ E-mail from Michal Slivovic, Director of Department of States of Eastern Europe, Southern Caucasus and Central Asia (8 November 2022) (on file with author).

¹⁰⁰ Eur. Ct. H.R., O.J. (L 323/66), https://www.echr.coe.int/Documents/HUDOC_38263_08_Annexes_ENG.pdf

¹⁰¹ It was on 20th–30th place in readership of online media in 2023. Jaroslav DANIŠKA: Dobrá správa: čítanosť a vplyv Štandardu rastú. *Standard.sk*, 19 June 2023. <https://standard.sk/373242/dobra-sprava-citanost-a-vplyv-standardu-rastie>

tablished moderate conservative-national online newsportal (the second one is *Postoj.sk* which means both ‘Attitude’ and ‘Wait a moment’) was rated at *Konspiratori.sk* portal among highly problematic outlets, with a negative rating 6.9 out of 10 points. This was followed by an extensive (detailed) public exchange of opinions among editors at *Standard.sk*,¹⁰² supported by editors of *Postoj.sk*,¹⁰³ with the author of this negative assessment.¹⁰⁴ Based on this exchange of opinions and arguments, it is highly questionable whether NGO Konšpiratori.sk had developed and applied really fair and persuasive enough methodology for classifying online outlets as ‘controversial’.

5. Conclusions

As can be seen, the fight against disinformation is rather complex and controversial from legal-constitutional or other perspectives. Enormous human and financial resources have been invested in this field. In three years, at least three different draft laws which were intended to tackle disinformation with a more multi-faceted approach were produced by two ministries (not to mention individual or group initiatives by MPs). Yet, none of draft laws was passed in the end.

The new government has cancelled the Action Plan, and approved a new Concept of Strategic Communication in March 2024. In effect, there is shift from a very loose approach, represented by the important role of the NGOs, to a highly centralised approach, represented by the key role played by the Office of the Government. Moreover, an update to Act on Media Services, following the Digital Services Act, has granted new and important rights to the MSB with respect to content sharing platforms. However, some of these rights have only be in effect since June 2025.

The first real emergency intervention (justified by alleged national security issues) was to regulate controversial webportals which had allegedly disseminated online disinformation posing a national security risk. This was immediately heavily criticized and ended in fierce public legal debates about the constitutionality of such measures. As a result, the extension of legal option for the NSA to ban some controversial NSA ex officio was not approved beyond September 2022 by the Parliament in the summer of 2022. Therefore, the first ban of some controversial websites lasted only a few months during the spring of 2022. As of 2024, or since June 2022, no websites have been banned (except those regulated by EU-wide *ad hoc* emergency regulation of selected Russian websites). However, whether the NSA may actually still block some websites with controversial content on request by third parties remains untested. Some lawyers argue that such legal option does exist., but the NSA has not produced an unambiguous statement in that regard: it merely copied the text of the law, law which remains blurred on this point.

¹⁰² Peter ŠTEVKOV: Analýza Štandardu. Prečo Konšpiratori.sk nehovorí pravdu. *Standard*, 6 December 2023. <https://standard.sk/511125/analiza-standardu-preco-konspiratori-sk-nehovoria-pravdu>

¹⁰³ Martin HANUS: Týždenný výber šéfredaktora. Ako prvé ruší Fico IV. najkonzervatívnejšiu reformu bývalej vlády. *POSTOJ*, 13 November 2023. <https://www.postoj.sk/141573/ako-prve-rusi-fico-iv-najkonzervativnejšiu-reformu-byvalej-vlady>

¹⁰⁴ Pavol HARDOŠ: Posudok – standard.sk. 2023. <https://konspiratori.sk/stranka/1250>

For the NSA to act, it would need to follow all administrative-legal steps in the procedures, which seems to be impossible at the moment due to confusing and contradictory legal regulations. Even the public media discourse seems to suggest that the NSA is not allowed to block any controversial content at all.¹⁰⁵ The new government appears to be unlikely to welcome or to support such ban being issued or tested by the NSA on request by a third party. For example, Matúš Šutaj Eštok, the minister of interior, participated in an online discussion lead by Daniel Bombic *aka* Danny Kollar in March 2024. At that time, Bombic was subject to three international warrants due to dissemination of extremist materials, cyberbullying and making public private data. He was living in the UK and faced extradition requests the same month. Moreover, this debate was co-moderated by Judita Laššáková, then candidate for Smer-SSD for elections to the European Parliament (elected). The British lower court approved extradition of Bombic in April 2024, subject to appeal.¹⁰⁶

Some educational and analytical outputs produced by analysts and activists contribute to spreading disinformation rather than to rational debate or to fighting disinformation. Some state authorities, and some diplomats also disseminate or support public dissemination of misinformation. The Police have also become involved in the controversial fight against misinformation and disinformation. Ironically, some new MPs, including new minister of culture, Martina Šimkovičová, gained their popularity (which translated into success in general elections) from being active on or appearing on some webportals listed as controversial and on alternative media such as online TV Slovan.

On the other hand, ‘alternative’ webportals (or social media for that matter) do not represent quality journalism or an ideal space for rational debate about public affairs. As mentioned, the efforts of some controversial webportals to fight back legally against being publicly listed as ‘conspiratory-like’ sources has not succeeded. Although, it should be mentioned that they have attempted to use rather innovative argumentation legally speaking. Their argumentation was based – in addition to standard legal arguments such as being under some kind of libel attack – on business law arguments (i.e. that the media-business competition was trying indirectly to destroy/damage their reputation, using unfair methods). Some of these cases are still awaiting a final judicial verdicts

In summary, although misinformation and disinformation is indeed a problem in Slovakia, no solution has been found that would tackle this issue effectively and efficiently, either from a legal perspective or from another (e.g. educational, analytical, monitoring) perspectives. Perhaps the only partial exception was the relative success in stopping deepfake video disseminated shortly before the 2023 general elections. It appears that approaches to fighting disinformation are based on dubious assumptions – that propaganda can succeed on its own under normal conditions within the population at large, without having met any necessary pre-conditions (such as

¹⁰⁵ See TASR: NBÚ od októbra nemôže blokovať škodlivý obsah, zákon nestihli prijať. *Teraz.sk*, 30 September 2022. <https://www.teraz.sk/slovensko/nbu-od-oktobra-nemoze-blokovat-sko/663946-clanok.html>; TASR: NBÚ od októbra nemôže blokovať škodlivý obsah, doteraz blokoval štyri weby. *Postoj*, 30 September 2022. <https://www.postoj.sk/115351/nbu-od-oktobra-nemoze-blokovat-skodlivy-obsah-doteraz-blokoval-styri-weby>

¹⁰⁶ Šimon KÉRY: Londýnsky súd rozhodol o osude extrémistu Bombica. „Som vydaný, prehrál som,” oznámil. *StartitUp*, 24 April 2024. <https://www.startitup.sk/londynsky-sud-rozhodol-o-osude-extremistu-bombica-som-vydany-prehral-som-oznamil/>

a very low mutual trust in society in general and in particular, towards institutions,¹⁰⁷ poor media literacy and general low knowledge levels among segments of the population, combined with real or imagined threats, with all this facilitated by occasional biased reporting from major media, occasional biased communication by ‘standard’ politicians and diplomats, and social media algorithms). Mesarčík identified sociological factors that either cause or facilitate disinformation (in addition to technical and economic factors) including: decrease of social capital (i.e. trust), increase in social inequality, increase in social polarisation, distrust in science, and evolution of media environment. Indeed, ‘alternative’ media and social media are part of the problem rather than a solution to it.¹⁰⁸

References

- 2MUSE (2021) = 2MUSE: *Dezinformácie a regulácia sociálnych sietí. Prieskum realizovaný pre europoslancu SPOLU / EPP Vladimíra Bilčíka*. https://europske.noviny.sk/wp-content/uploads/2021/12/Prieskum_2muse_Bilcik.pdf
- ANDERSON (2021) = Christopher William ANDERSON: Propaganda, misinformation, and histories of media techniques. *Harvard Kennedy School (HKS) Misinformation Review*, Vol. 2., No. 2. (2021) <https://doi.org/10.37016/mr-2020-64>
- ANSTEAD (2021) = Nick ANSTEAD: *What do we know and what should we do about...? Fake news*. Thousand Oaks, Sage, 2021. <https://doi.org/10.4135/9781529738896>
- CHLEBCOVÁ HEČKOVÁ – SMITH (2023) = Andrea CHLEBCOVÁ HEČKOVÁ – Simon SMITH: Slovakia. In: Nic NEWMAN – Richard FLETCHER – Kirsten EDDY – Craig T. ROBERTSON – Rasmus Kleis NIELSEN: *Digital News Report 2023*. Oxford, Reuters Institute, 2023. 96–97. <https://doi.org/10.60625/risj-p6es-hb13>
- HAJDU et al. (2023) = Dominika HAJDU – Jana KAZAZ – Katarína KLINGOVÁ – Patrik SZICHERLE – Viktória MUSILOVÁ: *GLOBSEC Trends 2023. United we (still) stand*. Bratislava, Globsec, 2023. <https://www.globsec.org/what-we-do/publications/globsec-trends-2023-united-we-still-stand>
- HAJDU–KLINGOVÁ (2020) = Dominika HAJDU – Veronika KLINGOVÁ: *Voices of Central and Eastern Europe. Perceptions of democracy & governance in 10 EU countries*. Bratislava, Globsec, 2020. <https://www.globsec.org/sites/default/files/2020-06/Voices-of-Central-and-Eastern-Europe-read-version.pdf>
- HAMID (2022) = Nafees HAMID (2022): *Mass media and persuasion. Evidence-based lessons for strategic communications in CVE. Briefing Note*. London, King’s College, 2022. https://www.xcept-research.org/wp-content/uploads/2022/07/2022-07-19_FINAL_Briefing-note-Mass-media-Jul19.pdf

¹⁰⁷ A Czech study has found that only low trust in institutions correlates with conspiratory vision of the world. See <https://www.irozhlas.cz/neduvera> (the full report is not officially available).

¹⁰⁸ MESARČÍK (2023), 38.

- HRCKOVA et al. (2022) = Andrea HRCKOVA – Robert MORO – Ivan SRBA – Jakub SIMKO – Maria BIELIKOVA: Autonomation, not automation: Activities and needs in European fact-checking organizations as a basis for designing human-centered AI systems. *ACM Journal on Responsible Computing*, Vol. 2., No. 4. (2022) Art. no. 17. 1–42.
<https://doi.org/10.1145/3764592>
- HUSOVEC (2022) = Martin HUSOVEC: Súčasné blokované dezinformačných stránok je ústavne problematické. Čo s tým? [The Current Blocking of Disinformation Sites is Constitutionally Problematic. What About That?] *DenníkN*, 222 April 2022.
<https://dennikn.sk/2818631/sucasne-blokovanie-dezinformacnych-stranok-je-ustavne-problematicke-co-s-tym/>
- KOLTAY (2023) = András KOLTAY: Censorship as a tool against state disinformation. The freedom of expression implications of the Russian–Ukrainian war. *Journal of International Media and Entertainment Law*, Vol. 10., No. 1. (2023) 1–53.
<https://www.swlaw.edu/sites/default/files/2024-01/JIMEL%2010.1%20Koltay231215.pdf>
- LANGER (2023) = Tomáš LANGER: *Case study slapp in Slovakia*. Bratislava, MEMO 98, 2023.
https://memo98.sk/uploads/content_galleries/source/memo/patfox_2022/slovakia-case-study-en.pdf
- MESARČÍK (2023) = Matúš MESARČÍK: *Nástroje verejného práva pre boj s dezinformáciami v online prostredí*. Bratislava, Právnická fakulta Univerzity Komenského v Bratislave [Comenius University Faculty of Law], 2023. https://www.flaw.uniba.sk/fileadmin/praf/Pracoviska/Ustavy/UPITPDV/E-KNIHY/Monografia_mesarcik_01.pdf
- OSMUNDSEN – BANG PETERSEN – BOR (2021) = Mathias OSMUNDSEN – Michael BANG PETERSEN – Alexander BOR: How partisan polarization drives the spread of fake news. *Brookings*, 13 May 2021. <https://www.brookings.edu/articles/how-partisan-polarization-drives-the-spread-of-fake-news/>
- PISKLOVÁ–SÝKORA (2021) = Miroslava PISKLOVÁ – Juraj SÝKORA: Disinformation and the Slovak Republic. In: Miroslava PISKLOVÁ – Juraj SÝKORA (Eds.): *Disinformation and the V4*. Bratislava, Slovak Foreign Policy Association, 2021. 3–10.
<https://www.sfpa.sk/wp-content/uploads/2021/08/Disinformation-and-the-V4.pdf>
- PIŠKO (2020) = Michal PIŠKO: Dezinformačné weby pravidelne číta každý siedmy. *Transparency International Slovensko*, 20 February 2020.
<https://transparency.sk/sk/dezinformacne-weby-pravidelne-cita-kazdy-siedmy/>
- SIMKO et al. (2022) = Jakub SIMKO – Patrik RACSKO – Matus TOMLEIN – Martin HANAKOVA – Robert MORO – Maria BIELIKOVA: A study of fake news reading and annotating in social media context. *arXiv:2109.12523v2* [cs.HC].
<https://doi.org/10.48550/arXiv.2109.12523>
- ŠKOLKAY (2018) = Andrej ŠKOLKAY: A case-specific instance of media capture. The Gorilla Case of Slovakia. *Środkowoeuropejskie Studia Polityczne*, No. 4. (2018) 65–94.
<https://doi.org/10.14746/ssp.2018.4.4>

- ŠKOLKAY (2022) = Andrej ŠKOLKAY: *Journalism and Populism in Slovakia, National Riport. DEMOS Project. Work Package 7, Task 7.3, Version 2.* Bratislava, School of Communication and Media, 2022. http://www.skamba.info/wp-content/uploads/2022/03/Task_7_3_National_reportsLOVAKIAmediaPopulism-10.11-4.pdf
- SPOHR (2017) = Dominic SPOHR: Fake news and ideological polarization. Filter bubbles and selective exposure on social media. *Business Information Review*, Vol. 34., No. 3. (2017) 150–160. <https://doi.org/10.1177/0266382117722446>
- ŠTEPANOVIČ (2021) = Dominik ŠTEPANOVIČ: Cena za (dez)informácie. *Výnosy z reklám webov s problematickým obsahom. Komentár č. 1-2021.* Analytical Department of Ministry of Defence, April 2021. https://www.mosr.sk/data/files/4364_2021-k-01-cena-za-dezinformacie-recenzovane.pdf
- URSPRUNG (1994) = Tobias URSPRUNG: The use and effect of political propaganda in democracies. *Public Choice*, Vol. 78. (1994) 259–282. <https://doi.org/10.1007/bf01047758>