Chapter VIII

The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism in Slovakia

Gábor Hulkó

1. Introduction

The technological capabilities of Internet communication, the existence (or non-existence) of constitutional foundations for social media, and whether state regulation, self-regulation, and national or global regulations are appropriate for social networks are not yet clear. State action is limited by the jurisdiction system, and in the case of the global self-regulation of service providers, no rule of law guarantees the restriction of fundamental rights. In many cases, such laws are arbitrary.[1]

When considering the state regulation of social media, it is worth distinguishing two problems: *the assessment of disputes and legal liability between users* and *the legal liability of platforms.* In the case of the settlement of disputes between users, in the countries examined in this study, users can sue each other in the same way as in the offline world, or they can conventionally accuse if they suspect that a crime has been committed. The legal procedures remain the same, but the specifics of communication on the social media platform must be considered when investigating an infringement.[2] *The regulation*

1 Klein, 2018, p. 38.
2 Koltay, 2019, p. 14.

Gábor Hulkó (2021) The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism in Slovakia. In: Marcin Wielec (ed.) *The Impact of Digital Platforms and Social Media on the Freedom of Expression and Pluralism,* pp. 245–276. Budapest–Miskolc, Ferenc Mádl Institute of Comparative Law–Central European Academic Publishing.

https://doi.org/10.54237/profnet.2021.mwsm_8

of the liability regime for content on social media platforms is another matter and raises different questions: first, the responsibility of social media platforms for user-uploaded content; second, the reaction of social platforms to this uploaded content: whether they ban users' posts and delete (censor) information. In this regard, social media platforms can influence the flow of information at the local or global level; thus, they *de facto* intervene with individuals' freedom of expression and right to information.

2. Regulatory and institutional framework of freedom of expression and censorship in Slovakia

Democratic society and the rule of law guarantee every individual the right to express their views orally, in writing, in print, through images, or otherwise and freely seek, receive, and impart ideas and information, regardless of national borders. *Freedom of expression and the right to information are guaranteed in Art. 26 of the Constitution of the Slovak Republic*,[3] and their limitations and obligations are also stipulated by law. These rights can only be restricted 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 public health and morality.[4] Public authorities are obliged to provide information about their activities in the state language in an appropriate manner, while the conditions and manner of implementation are established by law.

The Slovak legal system respects the protection of personal data and provides restrictions on access to or non-disclosure of information, such as possible infringements of intellectual property protection or concerns about decision-making by courts or law enforcement agencies. Restrictions have also been established for other special regulations. *Regarding the conflict and realization of the rights to information and protection of personality, one must be limited in favor of preserving the other.* A special status is acknowledged for public figures and representatives of state power for whom the limits of admissible criticism are extended—the expression of critical opinions about the behavior of certain individuals must be allowed within the enwidened boundaries of freedom of expression.[5]

Freedom of expression guarantees the right of citizens to express their thoughts and opinions, which can only be restricted by law. According to the Slovakian constitutional approach, it is a human right. More *precisely, it is a political right that ensures the dissemination of different political views and allows citizens to influence*

3 *460/1992 Zb. Ústava Slovenskej republiky.* Available at: https://bit.ly/2YNuYU5.

4 Constitution, Art. 26(4).

5 Representatives of state power or public figures must realize that when obtaining this status, the rules also include certain restrictions on their rights to private life, and they may be the subject of wider and sharper criticism in the public interest and the interest of their political opponents.

political developments in the state and participate in public events. Further, it allows protest rallies to take place and uncensored public information on public affairs to be disseminated, as well as the confrontation of the thoughts of an ordinary citizen with the attitudes and opinions of other people. As the freedom of each individual ends where the right of another begins, freedom of speech cannot be abused to interfere with the right of another person. Negative information, even if untrue, can reduce a person's credibility in society and authority in the workplace and disrupt their social relationships. *The provision of false information about events and the abuse of freedom of expression to commit violence are prohibited.*

Everyone is a holder of the right to freedom of expression—not only a natural person but also a legal person, a stateless person, or a group of persons without legal personality (petitions committees, party preparatory committees, and consortia). Every subject to the right to freedom of expression falls under the protection guaranteed by Art. 26 of the Constitution.[6]

The *Constitution of the Slovak Republic*[7] *defines cases in which freedom of expression may be restricted* and sets three basic conditions: a) the restriction of freedom of expression is defined by law[8]; b) a legitimate purpose of the protection of public or individual interest (the protection of the rights and freedoms of others, security of the state, public order, protection of public health and morals); c) the restriction can be considered a measure necessary in a democratic society. This restriction is possible only within the meaning of Art. 26 (4) of the Slovak Constitution by law, on constitutional grounds.

The fundamental principles of the liability system of social media platforms are based on freedom of expression and constitutional rules concerning access to information. Slovakian regulations do not distinguish between online and offline "forums"—*the medium through which the expression of opinion takes place is irrelevant.* Taking a general approach, several aspects of legal responsibility for expressing opinions can be distinguished on online interfaces. In the case of the *private law aspect* of an infringement, the right of privacy is typically violated: this may involve an interference with some personal data, violation of human dignity, privacy, or defamation. These cases typically comprise disputes between individuals ultimately decided by a court. *From a public law perspective*, we can distinguish between administrative-type violations and related administrative sanctions, and in more serious cases, criminal acts and penalties. Administrative-type infringements in Slovakia typically include personal data protection and conflicts of expression, in which case the data protection authority acts in public proceedings and may impose administrative measures and fines. The subject of these proceedings is the protection of personal data, but it does not exclude the possibility of enforcing damages in a civil law procedure. Similarly, in other administrative

6 Filip, 1998, p. 625.

7 Constitution, Art. 26.

8 For instance, criminal acts involving racist statements, symbols of fascism, or lies with the intention of harming others.

sectors, freedom of expression may conflict with other rules and prohibitions. A further public-law restriction on freedom of expression is the framework established by criminal law. In particular, the current criminal Slovak law categorizes hate speech as other types of criminal acts (incitement against the community, use of an authoritarian symbol, or incitement to violence). Nevertheless, it is possible to differentiate the *legal means of protection in case of abuse of freedom of expression* as follows: a*) civil law protection* (protection of personality, good reputation); b) *criminal protection* ("hate speech"); c) *administrative law protection* (broadcasting and retransmission regulation in media services, press regulation, or regulation on advertisements, consumer protection).

Censorship is also prohibited constitutionally: censorship is forbidden.[9] In the prevailing doctrine in Slovakia, the concept of "censorship" is only relevant in the relationship between state and freedom of speech—the regulation is directed toward the state and its organs (*de iure* censorship). Therefore, this constitutional rule does not apply to actions of private individuals or corporations capable of limiting, banning, or *de facto* censoring the views of others.[10]

From an institutional perspective, there is no state or administrative organ that actively and explicitly supervises the freedom of expression. However, regarding this fundamental right, several public administrations perform subtasks within their sector. These include, in particular, the Office for Personal Data Protection (*Úrad na ochranu osobných údajov*),[11] the Council for Broadcasting and Retransmission (*Rada pre vysielanie a retransmisiu*),[12] and the State Committee for the Supervision of Electoral and Political Party Financing (*Štátna komisia pre voľby a kontrolu financovania politických strán*).[13] Broadly, this also includes the Council of Slovak Radio and Television (*Rada rozhlasu a televízie Slovenska*),[14] which conducts public service media oversight. Overall, its task is to guarantee and control the independent operation of public service media and the provision of objective and balanced information.

The *Office of Personal Data Protection* is primarily responsible for state tasks in connection with personal data protection. Freedom of expression in the operation of this office is affected in the context of personal and protected data. The *Council for Broadcasting and Retransmission* performs certain state tasks in the field of radio and television. Its main mission is to promote public interest in the exercise of the right to information, freedom of expression, cultural values, and access to education in the sector, in particular licensing, supervision, sanctioning, and individual administrative tasks. The Council does not independently monitor the exercise of freedom of expression but may generally examine it (in the context of some

9 Constitution, Art. 26(3): Censorship is banned.
10 See below for more detailed elaboration on this matter.
11 Available at: https://dataprotection.gov.sk/uoou/.
12 Available at: http://www.rvr.sk/.
13 Available at: https://www.minv.sk/?statnakomisia.
14 Available at: https://www.rtvs.org/rada-rtvs/o-rade-rtvs.

other objective). The *State Committee for the Supervision of Electoral and Political Party Financing*—responsible for overseeing the financing of elections and political parties—is primarily involved in the financial oversight of party operations and the transparency of election campaigns. It may control freedom of expression only tangentially in its activities.

3. Constitutional and legal sources of the regulation of freedom of speech

Art. 26 of the Constitution of the Slovak Republic[15] provides a constitutional framework for freedom of expression (*sloboda prejavu*) and the right to access information (*právo na informácie*). Pursuant to Art. 26 (1), freedom of expression and the right to information are guaranteed in the territory of the Slovak Republic, enjoying constitutional protection. Accordingly, under para. 2, everyone has the right to express their views orally, in writing, in the press, through images, or otherwise and freely seek, receive, and impart ideas and information, regardless of frontiers[16]. Both freedom of expression and the right to information may be restricted, as stated above. The prohibition of censorship is stated in Art. 26 (3) of the Constitution.

Provisions more narrowly or broadly related to freedom of expression are contained in several pieces of legislation. These include, in particular, the following: provisions of the Civil Code (*zákon č. 40/1964 Zb. Občiansky zákonník*)[17] on personal rights, general liability and compensation; facts of the Criminal Code (*zákon č. 300/2005 Z. z. trestný zákon*)[18] concerning violations of the rules of community coexistence (e.g., incitement against a community, violence against a member of a community); Act no. 22/2004 on Electronic Commerce (*zákon č. 22/2004 Z.z. o elektronickom obchode*)[19]; Act no. 211/2000 on Free Access to Information (*zákon č. 211/2000 Z. z. o slobodnom prístupe k informáciám*)[20]; Act no. 18/2018 on Personal Data Protection (*zákon č. 18/2018 Z. z. o ochrane osobných údajov*)[21]; Act no. 185/2015

15 *460/1992 Zb. Ústava Slovenskej republiky*. Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1992/460/ (Accessed 31 May 2021).

16 Constitution, Art. 26(2): Everyone has the right to express their opinion in words, writing, print, images, or otherwise and seek, receive, and disseminate ideas and information freely, regardless of the state borders. No approval process shall be required for press publishing. Entrepreneurial activity in the field of radio and television broadcasting may be subject to permission from the State. The conditions shall be laid down by a law.

17 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1964/40/20191201.

18 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2005/300/20210101.

19 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2004/22/.

20 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2000/211/20210101.

21 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2018/18/20190901.

on Authorship (*zákon č.* 185/2015 *Zb. Autorský zákon*)[22]; Act No. 308/2000 on Broadcasting and Retransmission (*zákon č. 308/2000 Zb. o vysielaní a retransmisii*)[23]; Act no. 167/2008 on Periodicals and News Agencies (*zákon č. 167/2008 Zb. o periodickej tlači a agentúrnom spravodajstve*)[24]; Act no. 372/1990 on Misdemeanors (*zákon č. 372/1990 Zb o priestupkoch*)[25]; Act No. 351/2011 on Electronic Communication (*zákon č. 351/2011 Z. z. o elektronických komunikáciách*).[26] Another feature of the general legal framework is that the Slovak legislator has not yet implemented the 2018 amendments[27] to the AVMS Directive, which are listed in the legislative plan of the government.[28]

4. Legal sources and general rules of social media platforms

Social media platforms are *not specifically regulated* in the Slovak legal system. The only current regulation that has some direct relevance to social media liability (social media vs. state relation) is based on the abovementioned *Act No. 22 of 2004 on electronic commerce* (hereinafter referred to as the e-Services Act). This act was passed to transpose the rules of the e-Commerce Directive[29] into national law—*it is not targeted at regulating social media platforms specifically,* but it can theoretically also be applied to them.

Furthermore, Slovak legislation does not define a special concept of illegality or infringement, either in relation to e-services or social media. Accordingly, an infringement is considered to be any infringement under Slovak law. In the case of the removal of infringing content and the infringement suffered online, an individual can, as a general rule, *seek out a court*. In some branches, such as the protection of personal data and the protection of copyright, there is an administrative supervisory body. *Therefore, administrative intervention is also conceivable under sectoral legislation*. *The investigating authorities may act* on suspicion of a criminal offense. The regulation does not differentiate between infringements committed in

22 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2015/185/.
23 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2000/308/.
24 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2008/167/20191101.html.
25 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/1990/372/20210501.
26 Available at: https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2011/351/20210801.
27 Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities.
28 Available at: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2020-622.
29 Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce').

the "online" and "offline" space; thus, the nature of the medium is irrelevant to the availability of legal means. According to Slovak regulations, the individual layers of user-state-provider relationships in the online space can vary, as described below:

Relation type	**Example**	**Possible action/consequence**
a) user vs. user	personal right protection; copyright infringement; personal data protection	court and/or administrative action
b) user vs. state	hate speech or similar unlawful act (criminal acts, administrative offences)	police investigation, court and/or administrative action
c) user vs. provider	removal of users' content; alleged censorship	providers' terms and policies or court
d) provider vs. state	passive provider (e-Services Act); providers that commit unlawful acts	administrative or court action

Court procedures can occur in *a) user vs. user* disputes on social media platforms; however, for special violations (such as data protection and copyright violations), administrative procedures can be initiated, and administrative legal consequences are determined. The *b) user vs. state* relationship is mostly relevant in cases of serious breaches of the law (e.g., criminal acts), for which the police organs undertake the necessary means to stop such behavior. This can be followed by criminal court procedures. The *c) user vs. provider* relationship is considered a private contract between private individuals under Slovak law. Therefore, for unsolvable disputes under the terms of service (such as the removal or banning of users or their content and restricting users' information), the plaintiff can turn to court to resolve the issue. The liability of the *d) provider to the state* describes the responsibility for online content relayed and/or displayed by the provider. In the latter case, the service provider's liability for content is significantly limited and practically excluded. According to the law, the *service provider is not responsible for the transmitted information if the provision of the service comprises only the transmission of information in the electronic communications network or the provision of access to the electronic communications network*. Simultaneously, the service provider should not have a) initiated the transmission, b) selected the recipient of the information, or (c) compiled or modified the information. Furthermore, the service provider *shall not be liable* for information stored in the memory of the electronic devices used for information retrieval at the request of the user, *provided that the service provider is not aware of the illegal content of the stored information and takes immediate action to put an end to the user's unlawful conduct.* For such information, the service provider shall be liable only if the user acts on its instructions. In summary, *the service provider is responsible for the content it stores or transmits if*

a) it has become aware of its illegality and has not acted against it or if b) it has had a significant influence on the compilation of the information. With these provisions, the legislator transposes Art. 14 of the e-Commerce Directive into Slovak law with virtually no substantive changes.

Thus, it would be considerably difficult to hold the largest group of service providers liable for the information they store or transmit. Exceptions are news portals (online newspapers, magazines), online radios, and television channels—all service providers who produce their own information or news or have a significant influence on it. The forums of such providers are moderated posts that violate rights or public morality are removed, following the rulings of the European Court of Human Rights on October 10, 2013, in Delfi AS v. Estonia's[30] verdict.

Furthermore, *service providers have no obligations to monitor users' content, and the regulations explicitly prohibit the service provider from searching the data users transmit or save* without their consent. Nevertheless, if the provider becomes aware of the illegality of such information, it shall remove or at least prevent access to it, and the court may order the service provider to remove the information even if the service provider is unaware of its illegality. Thus, the search for user information is generally excluded, so the service provider *has no obligation to actively search for content (content tracking).*

Apart from political statements and newspaper reports,[31] there is *no common legal or scientific position* on the *obligation for social media platforms to intervene against illegal users' content,* nor *on the removal or banning of user-generated content,* except the e-Services Act Slovak. The literature cites the court case of *Stacho v. Klub Strážov,*[32] in which a comment on a website that violated the human dignity of a specific individual (not an article but a reader's comment) was disputed.

5. Content censorship in social networks in Slovakia

5.1. General rules on censorship

As stated above, the Constitution of the Slovak Republic prohibits censorship but does not define it. Likewise, the legal definition does not exist in any valid law. The only legal definition of the term was provided by the previous press regulation, Act no. 81/1966 on periodicals and other mass media (*zákon č. 81/1966 Zb. o periodickej tlači a o ostatných hromadných informačných prostriedkoch*): *Censorship refers to any intervention by state authorities against freedom of speech and image and their*

30 Delfi AS v. Estonia. Available at: https://bit.ly/2XmB2Te.
31 See: https://bit.ly/3zb9IUX and https://bit.ly/2XkaNw8.
32 Husovec, 2012.

dissemination by mass media. This is without prejudice to the powers of the prosecutor and court.[33] As this is the only legal definition of the term included in the Slovak legal system, it remains relevant to date,[34] although it was replaced by the current regulations in 2008.

Without a *definitionem legis,* various attempts have been made to define. According to the prevailing theoretical approach, *censorship is an official examination of everything intended for publication (especially the press), considering state, political, and moral interests, including the possibility of an official ban on publication*[35]. The opposite side of censorship should also be considered, such as in cases in which the court in a personal protection dispute orders the defendant to refrain from making statements in the future that violate the plaintiff's right to protection of personality. Censorship is not a publisher's obligation to withdraw a book the content of which infringes on the personality or copyright of another person. In all such cases, these are measures taken by public authorities based on proceedings initiated in relation to specific subjective rights or public interests that are directly endangered[36]. *Inadmissible censorship includes institutional, preliminary (preventive), and subsequent censorship*.[37]

Furthermore, *self-censorship cannot be subsumed under the accepted definition of censorship in the sense of the Constitution*. This is also a relevant issue, as self-censorship refers not only to individuals' self-restraint in their writing or speech but also to an editor's refusal to publish anything in a newspaper or magazine or a publisher's requirement to edit a book not in conflict with copyright law.[38] Excluding this type of censorship "sweeps it under the rug," pretending there is no problem while it erodes freedom of speech.[39]

Most authors define relevant *conceptual features of censorship's public power nature—prohibition of censorship is addressed exclusively to the state*. Interference with freedom of expression by private individuals—while not necessarily less threatening than interference by public authorities—cannot be classified as censorship.[40] While most authors take this definition for granted, other approaches to this issue underline that the concept of "censorship addressed exclusively to the state" is outdated and should be revised. Forms of communication have changed and

33 See § 17 para. 2 of Act no. 81/1966. This regulation was in force only between June 28, 1968, and September 25, 1968. After September 1968, this para. was abolished and the definition never used again. See: https://bit.ly/3hVf0xQ.

34 Drgonec, 2015, pp. 61–79.

35 Bartoň, 2002, pp. 21–22.

36 Moravec, 2013, p. 34.

37 Pavlíček et al., 1999, p. 182.

38 Ibid.

39 In dealing correctly with the issue of freedom of expression, self-censorship may not be a sufficiently intense issue interfering with freedom of expression. It does not affect the mass media in the institutional sense and cannot be entirely neglected, as it represents a problem for freedom of expression at its core. See Drgonec, 2015, pp. 67–68.

40 Drgonec, 2015, p. 64.

developed drastically in the last two decades, and many communication platforms (such as social networks and mass media) no longer fit into the "traditional" concept of censorship. This creates a dangerous possibility that *de facto censorship, which shows all the hallmarks of censorship, will remain outside de jure censorship*—formal protection against censorship will be considerably remote material protection from censorship.[41] The half-a-century-old legal definition of censorship appears as if it is from another world because it comes from a completely differently organized Czechoslovak socialist state and society. Therefore, it should not automatically be used as the definition of censorship, which is the subject of Art. 26 par. 3 of the Constitution.[42] Censorship refers to the control of the content of disseminated information, the control of information sources, and institutionalization in the form of a submission and authorization obligation with the possibility of a power ban. This power is available to public authorities, the owners of mass media, and the employers of journalists as those affected by the speech. The ban on censorship is aimed at providing protection against censorship to any expression under constitutional protection.

5.2. Censorship in the decisions of the Constitutional Court

The interpretation of the constitutional provision on censorship is rather scarce in the legal practice of the Constitutional Court of the Slovak Republic. The latest decision considering the interpretation of Art. 26 par. 3 of the Constitution was Decision IV. ÚS 307/2014,[43] in which the Constitutional Court states that "Censorship (direct censorship) in the constitutional sense means mainly the *politically motivated intervention of public authorities in the freedom of expression* of the subject concerned. This comprises assessing the content of opinions, thoughts, ideas, facts, and their form of dissemination and representation intended by the subject, publisher, etc., in the future (ex-ante control) or which have already been made available to the public (ex-post control) to change or completely negate these views,

41 Arguably, "situations in which freedom of expression could be denied to an individual are constitutionally unacceptable because most other individuals can express an opinion without censorship. Everyone is subject to freedom of expression; therefore, everyone has the right to protection from censorship. The prohibition of censorship confers protection to every holder of the right to freedom of expression and the right to information. The prohibition imposed in the Constitution, protection against censorship, was granted in the highest available legal force. The constitutional ban on censorship is absolute and applies to all addressees of the ban. The Constitution does not grant an exception to anyone, nor does it exclude anyone from the circle of legal entities obliged to respect the prohibition of censorship. The strength of the traditions formed and formulated by the previous legal definition leads to a restrictive interpretation of the addressees of the ban on censorship, to their identification with the state authorities. Thus, the prohibition of censorship must be interpreted as one not addressed exclusively by a public authority but to any subject of law in a position of power." See Drgonec, 2015, pp. 61–79.

42 Drgonec, 2015, p. 62.

43 See: https://bit.ly/3nsuRrq.

thoughts, ideas, or facts or their form of dissemination and display, mainly for political reasons. *The nature of direct censorship can also impact freedom of expression comprising a ban on the dissemination or an additional ban on the dissemination of certain types of information that have been disseminated without restriction in the past* (e.g., a ban or additional ban on publishing, a ban or additional ban on the media, a ban on public publication). The reasons can be related to the subject or the content of disseminated opinions or ideas the subject concerned has in the past or at the time intended or disseminated unless it is prohibited for reasons justifiable by the Constitution."[44]

The Constitutional Court takes the same essential approach as the prevailing doctrinal view. Furthermore, in the aforementioned decision, the court only considers the definition and context of direct censorship and does not elaborate on other types of censorship. Despite the relevance of freedom of expression and its relationship with censorship in democratic societies and considering the consequences of censorship for the availability of freedom of speech, accessible legal literature and court decisions have focused on identifying the scope and content of the ban on censorship under Art. 26 par. 3 of the Constitution only marginally.

5.3. Censorship in social media

As the main legal doctrine of the ban on censorship in general aspects considers as "censorship" only actions with a nature of public power, there is no unified view on censorship of social media platforms. Slovak law only stipulates tangential rules on freedom of expression on the Internet and social media in certain provisions of the e-Services Act (as stated above), which may have a certain degree of applicability in this area. However, notably, this law was adopted to transpose the rules of the e-Commerce Directive into national law. This legislation is therefore not primarily intended to regulate online expression and social media but transposes the general liability of hosting providers laid down therein in accordance with the European Directive on Electronic Commerce. There is currently no legislative intention to regulate freedom of expression online or content removal of social media platforms.

The material scope of the e-Services Act is the information society services (*služby informačnej spoločnosti*). According to the regulations, such a service is any information society service provided *remotely* (e.g., the service is provided without the simultaneous presence of the parties), *electronically* (e.g., the service is sent from the point of origin and received at its destination entirely by wire, radio, optical, or other electromagnetic means), *usually for a fee* and *at the individual request of*

44 Ibid.

the recipient.[45] When examining the Slovak legislation, we can consider the general terms and conditions of service providers—bilateral private law agreements—to be of a "soft law" nature. The general approach to such contractual terms is that service providers reserve the right to remove infringing content, and the user can make court petitions to seek remedies.

In summary, as there is no regulation of social media platforms in Slovakia, *the system of public liability for content control by social media platforms is not stipulated in the Slovak legal system with regard to alleged or actual censorship*. Prohibiting the sharing of information or its removal from a particular medium may be ordered by a court, but service providers must remove the infringing content themselves. *The relationship between social media and the user is interpreted by Slovak law as a private law contract* within the framework of which the user consents to the service provider to remove certain (infringing) content. Thus, *if information (entry, comment) is deleted by the service provider, this can be challenged in court, but the Slovak legal system* does not provide other guarantees. In practice, such cases (in which the user files a lawsuit against social media platforms) do not occur.

6. "Fake News" and the influence of digital platforms and social networking on the guarantees of freedom of speech and truthfulness of information in Slovakia

There are currently no valid regulations of fake news in Slovakia. There were several instances in which the Slovak Police Force fought false information or misinformation about the latest COVID-19 measures in the country. This primarily included a heightened presence on the "official" social media channels of the force, in which constant and fact-checked information of the population was ensured. In parallel, false information and hoaxes were monitored, and the civil population was constantly informed about false news. There were also several cases in which interventions were taken against users from Slovakia for spreading false information on social media concerning the spread of the virus or the pandemic situation in general. These interventions were conducted among individuals who could be identified and tracked in Slovakia. These actions were undertaken in the context of the pandemic, and there are no known cases in which a social media platform

45 According to Slovak legislation, the provision of information society services in Slovakia does not require a permit or registration (notification). However, the provision of the service may be restricted if the service provider violates the requirements of state security, public order, public health, or environmental and consumer protection.

or other service provider was encouraged to ban users' posts or users on behalf of the police.

However, the Slovak government fully realizes that advances in information technology have provided citizens with access to extensive information and the creation of information. Much of such information is often misleading and/or untrue. The massive spread of various misinformation is increasing as one of the means of the "hybrid war." Such information operations are not new, but with the emergence of new platforms and more effective dissemination techniques, their impact on state security is rapidly increasing. As government documents state, *the term disinformation has not yet been codified in the Slovak legal system*. Simultaneously, disinformation can be considered part of a broader process called information operations in terms of information manipulation. The public is also exposed to the growing dissemination of dangerous rumors, misleading information, and conspiracy theories that can endanger human health, harm the cohesion of society, or lead to public violence and social unrest. *In addition to the targeted dissemination of potentially harmful information, information operations may involve the collection of sensitive data*, encourage people to take action (violent or non-violent), and openly or covertly promote a party or state.[46] Information operations have become the most frequently used hybrid indicator—not only of foreign actors—within the hybrid threat.[47]

In December 2018, the European Commission presented an *Action Plan to Combat Disinformation,*[48] the main aim of which was to strengthen existing mechanisms and build new ones to eliminate this dangerous phenomenon, including the use of artificial intelligence. The need for cooperation in the fight against misinformation within the EU is also one of the objectives of the forthcoming *European Democracy Action Plan*.[49] In this context, the results of the Eurobarometer[50] are alarming and present an argument in favor of addressing the issue, as 83% of respondents described online misinformation as a threat to democracy, a view consistent in all EU countries. At least half of the respondents stated that they encountered disinformation at least once a week, with the most positive answers recorded in Spain, Hungary, Croatia, Poland, France, Greece, and the Slovak Republic.

Official sources imply that *the Slovak government sees information operations as the greatest risk to national security*, as they can be conducted by foreign state and non-state actors (also by domestic actors who sympathize with the attacker). Sophisticated strategies are often taken to influence public debates, deepen the polarization

46 Such a systematic use of information operations is included among the hybrid indicators, which can become hybrid threats.

47 For details, see: https://bit.ly/2XdiAMZ.

48 Available at: https://bit.ly/391iSsf.

49 Available at: https://bit.ly/3EgIeRl.

50 On the final results of the Eurobarometer on fake news and online disinformation, see: https://bit.ly/2YJrp18.

of society, and create a growing group of people who do not trust any official source and are thus more easily manipulated. The result is a more effective intervention in democratic decision-making, the relativization of the country's political leadership, and the weakening of society's confidence in democratic institutions. *The role of the state and its competent components is to create a mechanism to eliminate the impact of disinformation campaigns*, especially through the effective identification of manipulative content and strategic communication.[51]

According to these findings, *the Slovak government's official perspective is that the state must strengthen its means and capacities for resilience to information operations* and cooperate with experts from the public and private sectors *to detect and analyze false information*. In its *program statement, the Government of the Slovak Republic*[52]*undertook to prepare an action plan for the coordination of the fight against hybrid threats and the spread of disinformation and build adequate central capacities for its implementation*. However, these steps must be in accordance with human rights legislation and must never weaken freedom of speech and the unrestricted access to information, which are basic human freedoms guaranteed by the Constitution of the Slovak Republic.

Realizing state security risks, the Slovak government has prepared a novelization of *Act no. 69/2018 on cyber security*[53] and an *administrative action plan*[54] (a coordinated mechanism of the Slovak Republic's resilience to information operations). In particular, the latter provides detailed insights into measures that the government plans to implement in this field.

6.1. The concept of state intervention against "Fake News" in Slovakia

6.1.1. General concepts regarding harmful information

In the context of the dissemination of potentially harmful information, there are numerous *elements of information operations*—activities or methods of implementation (hereinafter referred to as the "EIO"). The most well-known and most frequently used EIOs include the following:

a) *False reports* (fake news) comprise information that intentionally mimics the format of a news or other journalistic product, with its creators deliberately misleading their audiences by distorting reality.
b) *Hoax* includes deceptions, jokes, and virally extended alarm messages. They usually have three features: urgency, reference to illusory authority (such as police sources and scientific results), and requests for dissemination. A common intention is to cause fear or anxiety.

51 Ibid.
52 See: https://bit.ly/3htezKS.
53 See: https://bit.ly/395ao3C.
54 See: https://bit.ly/3AfltuY.

c) *Propaganda* includes information, ideas, opinions, or visual materials created and distributed to influence people's opinions. Propaganda is based not only on half-truths or untruths but also on facts, but it is always biased toward promoting a certain party or opinion. The intent is to induce objectivity despite the one-sidedness of the narrative, the aim of which is to convince and not inform.
d) *Conspiracy theory* explains an event or set of circumstances as a result of a secret conspiracy, usually by a small, powerful group of people. Such a group is usually the government, representatives of secret societies, organizations, or intelligence services, one or more cooperating companies or representatives of states, nations, or religions, or even extraterrestrial civilizations. Conspiracy theories reject the generally accepted explanations of these events.
e) *Parody and satire*, in the context of information operations, are used to disseminate misleading information aggressively or ridicule or criticize a goal (such as a person, group of people, or opinion) that goes beyond the ordinary framework of this genre.
f) *Disinformation* refers to false or manipulated information intentionally disseminated to mislead and harm. Disinformation can be false or manipulated texts, images, videos, or sound, and used to support conspiracies, spread doubts, and discredit true information or individuals and organizations. True information can also be classified as misinformation if presented in a manipulative manner. Misinformation does not include unintentional errors in news, satire, parody, or one-sided reports and comments clearly marked as such.
g) *Malinformation*[55] is based on reality and is intentionally disseminated to harm a person, organization, or state (e.g., leaked information, hate speech, or harassment).[56]

6.1.2. State aims and institutional provisions

The main aim of fighting harmful information on social media platforms is *to reduce and possibly eliminate the space and opportunities* for false and misleading information or news in all areas of public power and achieve society-wide awareness. Thus, it increases public confidence in public authorities, *increasing media literacy* and promoting an information source for objective journalism *to promote more active cooperation and information exchanges.*

55 Malinformation differs from misinformation, which is erroneous or false information spread unknowingly and without intent to harm. Therefore, it is not considered an element of information operations.

56 Council of Europe (2017) Report on Information Disorder: Toward an interdisciplinary framework for research and policy making, DGI(2017)09. Available at: https://bit.ly/2XdHkVl.

The individual state administration bodies of the Slovak Republic have planned a coordinated complex approach at both the vertical and horizontal levels of government and through intensive exchanges of information. The hypothetical goal of the regulation and administrative actions is to establish a consistently well-informed public, for which the government and all organizations and bodies in the public sector are responsible.

Preventive and directly performed activities in the Slovak Republic are planned to be guaranteed by the Government of the Slovak Republic and individual central state administration bodies. The *Situation Center of the Slovak Republic* (hereinafter referred to as "SITCEN")[57]—organizationally integrated into the structure of the Government Office of the Slovak Republic[58] (hereinafter referred to as "Central Office")—will have a specific position in the analysis of the identified elements of information operations (EIO). As part of the institutional system, the *National Security Analysis Center* (hereinafter referred to as "NSAC")[59]—a part of the Slovak Information Service[60]—will play an important role in this analysis, using input from the participating ministries. If it is found that the EIO meets the elements of the factual nature of the crime, the procedure will be left to the law enforcement authority (police organs and prosecutors' offices). Entities operating in the non-governmental sector are also significant in the prevention and identification of EIOs. The state will create a scheme for their involvement and financial support.

According to the administrative action plan, the main *SITCEN* tasks will be as follows: *a)* publish ongoing EIOs of a worrying, high, and critical level of influence and confront it with relevant facts, in consultation with the NSAC; *b)* provide official, comprehensive relevant information on EIOs; *c)* process, analyze, and evaluate EIOs; *d)* use designated software to work with information, obtaining and collecting EIOs, creating analyses, and advancing acquired EIOs; *e)* cooperate with non-governmental organizations and other entities to strengthen the prevention of EIOs; *f)* cooperate with foreign partners to identify possible international cases; *g)* maintain a database of assigned EIOs that may be useful in formulating media outcomes; *h)* cooperate in the development, updating, and use of disinformation software and provide support for public authorities involved in the use of the software; *i)* propose appropriate measures and guidelines to eliminate the spread of EIOs; *j)* contribute to raising awareness of the harmful effects of EIOs and their prevention; *k)* support practical training and education in the field; *l)* to organize conferences to evaluate EIOs over the past year, in the context of prevention, in cooperation with the academic and scientific community and non-governmental sector; *m)* cooperate with the

57 See: https://bit.ly/2VFUVUw.

58 More precisely, it is part of the Office of the Security Council of the Slovak Republic, an organizational part of the Government Office of the Slovak Republic. See: https://www.vlada.gov.sk//bezpecnostna-rada-sr/.

59 See: https://www.sis.gov.sk/o-nas/nbac.html.

60 See: https://www.sis.gov.sk/about-us/introduction.html.

media through consulting and training to keep it informed to eliminate or minimize the spread of EIOs.

The work of the SITCEN will be supported by *NSAC*, and both organizations will coordinate their activities in the field. The main competences of NSAC (which is a part of the intelligence services, as stated above) will be to *a)* cooperate with SITCEN to analyze EIOs, *b)* deliver an opinion according to the level of influence of the EIO, and *c)* in the case of critical EIOs, decide on the course of action.

The proposed material also defines tasks for other *organs of central administration*: a) search and assess EIOs in their area of responsibility manually, analytically, or through specially designed search software; b) prepare a description of the situation and identify the level of the EIO's influence; c) take a position on identified EIOs; d) forward all relevant information to the EIO to SITCEN; e) provide, within their respective spheres of competence, cooperation and additional information on the transferred EIO for SITCEN and NSAC; f) use dedicated, unified software to work with information, obtain and collect EIOs, create analyses, and forward acquired EISs to SITCEN and NSAC; g) use the data from the analyses of their own EIOs and from the outputs of the SITCEN to improve their strategic communication as a basic means of resilience to EIOs.

This institutional framework is supplemented by cooperation with non-governmental organizations, in which *selected non-governmental organizations* will be involved in the possibility of searching for EIOs (also possibly with the use of a designated software for this purpose, for gathering, analyzing, and forwarding EIOs to competent organs) and conducting educational activities.

6.1.3. EIO assessment criteria and state response

In assessing the level of impact, the assessor shall consider the following criteria: *a) the potential to cause harm* (manipulation, polarization of society, human health, economic damage, the rule of law, the credibility of the state); *b) the existence of the potential to provoke action* (non-violent, violent, mass unrest); *c) the size of the group that could be affected* (individual, small group, large group, whole population); *d) originator of the EIO* (individual, group, risk group, non-governmental organization, state organization, state representative); *e) the significance of the influence* of the status of the addressee and *the potential for amplification* (ordinary citizen, member of the risk group, generally recognized personality, civil servant, public prosecutor); f) the degree of probability of influencing the addressee (EIO content quality – *ability to convince the addressee*); g) *credibility of the EIO*; h) *coordination of the dissemination* (unorganized/organized); *i) the EIO's channel in terms of persuasiveness* (oral, social networks, website, print medium, audio visual medium); *j) the disseminator* (individual, group, risk group, non-governmental organization, state organization, state representative); *k) geographical source* (foreign, domestic); *l) characteristics of the conduct showing signs of crime* (defamation, dissemination of an alarm message, incitement to racial, religious or other intolerance); *m) existence*

of neutralization mechanisms (there is/is not a possibility to take countermeasures); *n) other significant circumstances* (timing, concurrence with other elements of hybrid threats, etc.).

Based on these assessment criteria, *the EIO's impact level is defined* based on complex, quantitative, and qualitative analyses. After determining the level of impact, it is necessary for the competent central state administration body to select an adequate response and implement it—*the nature of the response should correspond to the specified level of impact*. As a general rule, the response is implemented by the organ responsible for the sector administration (e.g., in the case of false information about environmental issues, the Ministry of Environment should act; in the case of fake news about public health questions, the Ministry of Healthcare is the competent authority). Depending on the individual characteristics of the assessed EIO, the possible responses fall under the following categories:

a) Negligible influence: There is only a remote possibility that the EIO will have some consequence; there could be an unintentional error in communication or a misunderstanding. While the error can be eliminated, the harmful information cannot trigger action, and the impact can be refuted by verified and documented facts. If the relevant organizational unit evaluates the impact as negligible, the reaction will generally not be necessary. If the competent organ has doubts regarding the level of impact, it consults and coordinates with SITCEN. If SITCEN discovers additional facts, it may change the level of influence.

b) Worrying impact: There is a likelihood of an adverse consequence or the creation of space for the spread of EIO; there may be a risk of harm to the credibility and/or health of an individual or group, violations of law; usually there is unorganized coordination of EIO. In this case, the EIO refers to the SITCEN together with an analysis, the determined level of impact, a description of the situation, and the method of response. SITCEN is obligated to register the EIO in its database, evaluates it, and subsequently forwards all connected information and a description of the situation to the NSAC, which constructs its opinion. Subsequently, the opinion is forwarded through SITCEN back to the competent administrative unit. If the NSAC identifies a different level of impact, its response corresponds to the specified level of impact.

c) High impact: There is a high probability of an adverse event with an impact on the credibility of state bodies, organizations, threats to the health of a group of persons, and threats to the seriousness of a group of persons. The EIO has a high potential to trigger an action, and organized coordination of EIO dissemination was indicated. In the case of high impact, the process of reaction is the same, as in the case of a worrying impact.

d) Critical impact: There is a considerably high probability of an adverse event, a significant threat to the credibility of state institutions and their representatives, the security of the state, significant strategic interests of the state, the

existence of serious damage to the health of a group of people or their lives, high economic damage, endangered sovereignty, territorial integrity, the principles of democracy, and the rule of law. The EIO impacts the whole population with extremely high potential to trigger action; there is highly organized coordination of EIO dissemination. The EIO is caused by a state representative or a state institution; there is excessive room for uncontrollable dissemination. In the case of a critical impact, the EIO refers to the SITCEN from the competent administrative unit, together with an analysis, the determined level of impact, a description of the situation, and the method of response. In this case, the SITCEN is obligated to send the EIO to the NSAC for subsequent analysis, which will consider the need to take measures or convene the NSAC Council, which shall decide on further action.

6.2. The use of social networks in Slovakia[61]

Social networks have become a crucial phenomenon that significantly affects the entire Slovak society. In Slovakia, 86% of the population uses a social network at least once a month, and 61% of people use it daily. The use of social networks is one of the most common activities performed by Slovaks on the Internet.

Facebook is the most widely used social network in Slovakia. At least once a month, Facebook is used by up to 76% of the population of Slovakia, while daily usage is at 55%. Facebook is slightly more popular among younger people; with increasing age, the intensity of its use decreases. Even teenagers who also use many other networks use Facebook daily. Furthermore, Facebook is used by state organs for communication purposes.

Regarding other social media platforms, *YouTube* has versatile uses, although it can be used comfortably without creating one's own account and without using the "social" dimension. Nevertheless, YouTube is used by 78% of Slovaks at least once a month, with 31% of the population using it at least once a day. It its thus the most watched provider of video content in general, even compared to television broadcasting. *Instagram* has become the third most widely used network. Although its core use base is composed of the youngest age groups, Instagram has managed to bridge the generational barrier. At least once a month, Instagram is used by up to 42% of the population, and a fifth of the population (22%) use it daily. Instagram is used by up to 80% of those aged below 26 but only about 10% of those age above 60. Once the most popular social network in Slovakia, *Pokec*, has a lower but stable userbase. Pokec is still used monthly by 19% of the Slovak population, and less than 9% of the population logs onto Pokec daily. It is most often used by people aged 27–40. In addition to large social networks, narrower networks have been

61 This sub-chapter is based on *Koľko Slovákov je na sociálnych sieťach?* (March 2021). Available at: https://bit.ly/3k4V5y7. As well as on *Králi sociálnych sietí na Slovensku: Facebook, YouTube a Instagram* (May 2015). Available at: https://bit.ly/3tzAW6s.

identified in the Slovak market. *Pinterest* has a high penetration (just over 20% of monthly users), although only a small proportion of this are core regular users. *Tik-Tok* also has a growing relevance; Tik-Tok users are often children below 15 years of age (and therefore are not included in the survey). Therefore, the number of real users in the whole population is probably higher than that indicated above, although the use of this social network is gradually reaching higher age categories. At least once a month, 13% of the population of Slovakia use it daily, at approximately 5%. *Snapchat* in Slovakia is currently rather stagnant; it is used by 9% of Slovaks per month, only 3% on a daily basis, while users are exclusively people aged below 26 (the core of the user group are teenagers, similar to Tik-tok). *Twitter* is an interesting case study. While it is used intensively globally (approximately a quarter of the American population has a Twitter account, and the tweets of the former American president, Donald Trump, received global attention practically every day), in Slovakia, Twitter did not catch on. At least once a month, 13% of the population uses it, but less than 3% do so daily. Twitter is thus used extremely passively, and its influence in Slovakia is rather marginal; however, its users are typically better-off people of younger middle age with a higher income and a higher social status. At least once a month, 8% of the population of Slovakia visits the professional social network *LinkedIn*. The audio social network *Clubhouse*, which was given much attention in early 2021, has thus far attracted only a marginal proportion of the Slovak population.[62]

6.3. Legal liability of users and digital media platforms

In questions of legal liability connected to freedom of expression, false information (EIO) and social media platforms have relatively few special rules. As explained above, the legal tools at disposal are commonly used in non-online cases. Furthermore, *liability only applies to users* and those who create their content themselves *but not to social media platforms or internet service providers*, except the provisions of the e-Service Act. A debate arose around the aforementioned court case *Stacho vs. Klub Strážov*,[63] where the plaintiff sought an *apology from the operator of the website, the removal of the post, and damages of EUR 5,000*, and the court in the second instance did not approve damages for the plaintiff but ordered the operator of the website to remove an unlawful comment. In the first instance, the court decided to remove the comment and the compensation of damages for the plaintiff. The question is whether the website operator is responsible for the damages if it had not removed the comment based on the request of the plaintiff. The plaintiff argued that the operator should have acted solely on his request, as the unlawfulness of the comment was clear in his opinion, while the operator argued that he was not aware of the unlawfulness of the comment until the decision of the court in the first

62 Available at: https://bit.ly/3ljd57o.
63 See: Husovec, 2012.

instance. The dispute has yet to be resolved, as the case is at the Supreme Court with no final decision.

In accordance with this, three levels of liability can generally be defined in the Slovak legal system: civil, criminal, and administrative. As stated above, Slovak regulations consider the disputes between the user vs. user and user vs. provider to have basis in private (civil) law, in which legal disagreements are resolved by courts—if a dispute shows elements of criminal or administrative unlawfulness, then the organs of criminal investigation and/or administrative organs can be involved. Therefore, civil liability in this regard is governed by the same rules and regulations as offline cases. Furthermore, there are no known court cases concerning the removal of user posts (or banning users) by social networks.

6.3.1. Rules of criminal liability

The Act no. 300/2005 on Criminal Code (*zákon č. 300/2005 Z. z. Trestný zákon*) or in short: Criminal Code[64] enumerates several provisions that could be applied to natural persons for deeds, which were conducted on online forums. These criminal rules naturally represent restrictions against freedom of expression but are in accordance with constitutional provisions. Crimes that can be committed in online spaces are usually tied to the phenomenon of "hate speech," although this term is never used in legal sources in Slovakia. The crimes connected to users in social network activities are as follows: *a)* disseminating false news[65]; *b)* defamation of nation, race, and belief[66]; *c)* incitement of national, racial, and ethnic hatred[67]; *d)* violence against a group of citizens and against an individual[68]; *e)* supporting and promoting groups aimed at suppression of fundamental rights and freedoms[69]; *f)* manufacturing, possession, and dissemination of extremist materials[70]; *g)* defamation[71]; *h)* unauthorized use of personal data[72]; *i)* serious threats[73]; *j)* dangerous persecution[74]; *k)* harm done to the rights of another[75]; *l)* breach of confidentiality of spoken utterance and other personal expression[76]; *m)* condoning a criminal offense.[77] From this perspective, the following crimes are particularly relevant:

64 Ďuračová, 2005.
65 Section 361 of the Criminal Code.
66 Section 423 of the Criminal Code.
67 Section 424 of the Criminal Code.
68 Section 359 of the Criminal Code.
69 Section 421 of the Criminal Code.
70 Section 422a-422c of the Criminal Code.
71 Section 373 of the Criminal Code.
72 Section 374 of the Criminal Code.
73 Section 360 of the Criminal Code.
74 Section § 360a of the Criminal Code.
75 Section 375-376 of the Criminal Code.
76 Section 377 of the Criminal Code.
77 Section 338 of the Criminal Code.

a) *Disseminating false news* is committed by any person who deliberately creates serious concerns among the population of a certain location or at least a part thereof by disseminating false or alarming news or committing other similar acts capable of giving rise to such danger. The offender shall be liable to a term of imprisonment of up to two years. Any person who reports false or alarming news, or other similar acts referred to above, to a legal entity, the police force, another state authority, or the mass media, although they know that such news is false and may cause serious concerns among the population of a certain location or at least a part thereof, shall be liable to a term of imprisonment of one to five years. Furthermore, any person who, in a crisis situation—even through negligence—creates the danger of serious concern, a mood of despondency, or defeatism among at least a part of the population of a certain location by spreading false or alarming news, shall be liable to a term of imprisonment of between six months and three years.
b) *Defamation of nation, race, and belief* refers to public defamation of any nation, its language, any race or ethnic group, or any individual or a group of persons because of their affiliation to any race, nation, nationality, complexion, ethnic group, family origin, religion or because they have no religion. In this case, the sentence shall be a term of imprisonment of one to three years. The offender shall be liable to a term of imprisonment of two to five years if they commit the offense with at least two more persons, in association with a foreign power or foreign agent, in the capacity of a public official, under a crisis situation, or with a specific motivation.
c) *Incitement of national, racial, and ethnic hatred*: any person who publicly threatens an individual or a group of persons because of their affiliation to any race, nation, nationality, complexion, ethnic group, family origin, or religion, if they constitute a pretext for threatening on the aforementioned grounds, by committing a felony, restricting their rights and freedoms, or who made such restrictions, or who incite the restriction of rights and freedoms of any nation, nationality, race, or ethnic group, shall be liable to a term of imprisonment of up to three years. The same sentence shall be imposed on any person who associates or assembles with others with a view to committing the offense, which shall be liable to a term of imprisonment of two to six years if they commit the offense referred to in association with a foreign power or foreign agent, in public, with a specific motivation, in the capacity of a public official, in the capacity of a member of an extremist group, or in a crisis situation.
d) The crime of *incitement, defamation, and threatening persons because of their affiliation with a race, nation, nationality, complexion, ethnic group, or family origin* is constituted when a person publicly incites to violence or hatred against a group of persons or an individual because of their affiliation to any race, nation, nationality, complexion, ethnic group, family origin, or

their religion, if they constitute a pretext for the incitement on the aforementioned grounds, or defames such group or individual, or threatens them by exonerating an offence deemed to be genocide, a crime against humanity or a war crime, or an offence deemed to be a crime against peace, a war crime, or a crime against humanity, if such crime was committed against such group of persons or individual, or if a perpetrator of or abettor to such crime was convicted by a final and conclusive judgement rendered by an international court, unless it was made null and void in lawful proceedings, publicly denies or grossly derogates such offence, if it has been committed against such person or individual, shall be liable to a term of imprisonment of one to three years.

e) *Violence against a group of citizens or against an individual:* Any person who threatens a group of citizens with killing, inflicting grievous bodily harm, or other aggravated harm, or with causing large-scale damage, or who uses violence against a group of citizens, shall be liable to a term of imprisonment of up to two years. The offender shall be liable to a term of imprisonment of between six months and three years if they commit the offense with a specific motivation, in a more serious manner, or in public.
f) *Supporting and promoting groups aimed at suppressing fundamental rights and freedoms*: Any person who supports or makes propaganda for a group of persons or movements that, using violence, the threat of violence, or the threat of other serious harm, demonstrably aims to suppress citizens' fundamental rights and freedoms shall be liable to a term of imprisonment of one to five years. The offender shall be liable to a term of imprisonment of four to eight years if they commit the offense in public, in the capacity of a member of an extremist group, acting in a more serious manner, or in a crisis situation.
g) *Manufacturing, possession, and dissemination of extremist materials*: Any person who manufactures or disseminates extremist materials or participates in such manufacturing shall be liable to a term of imprisonment of three to six years. The offender shall be liable to a term of imprisonment of four to eight years if they commit the offense acting in a more serious manner, in public, or in the capacity of a member of an extremist group. In the case of possessing extremist material, the offender shall be liable to a term of imprisonment of up to two years.
h) *Defamation*: Any person who communicates false information about another likely to considerably damage the respect of fellow citizens for such a person, damage their career and business, disturb their family relations, or cause serious harm, shall be liable to a term of imprisonment of up to two years. The offender shall be liable to a term of imprisonment of one to five years if they commit this offense and cause substantial damage, by reason of specific motivation, in public or in business acting in a more serious manner. The offender shall be liable to a term of imprisonment of three to eight years if they commit

the offense and cause large-scale damage or causes another to lose their job, collapse their undertaking, or divorce their marriage.

i) *Unauthorized use of personal data*: Any person who, without lawful authority, communicates, makes accessible, or discloses personal data of another obtained in connection with the execution of public administration or with the exercise of constitutional rights of a citizen, or personal data of another obtained in connection with the execution of their own profession, employment, or function, and thus breaches their own obligation prescribed by a generally binding legal regulation, shall be liable to a term of imprisonment of up to one year. The offender shall be liable to a term of imprisonment of up to two years if they commit the offense and causes serious prejudice to the rights of the person concerned, in public, or in a more serious manner.

j) *Serious threats:* Any person who threatens another with killing, inflicting grievous bodily harm, or other aggravated harm to an extent that may give rise to justifiable fears shall be liable to a term of imprisonment of up to one year. The offender shall be liable to a term of imprisonment of between six months and three years if they commit the offense in a more serious manner, against a protected person, with the intention of preventing or obstructing the exercise of fundamental rights and freedoms by another, by reason of specific motivation, or in public.

6.3.2. Rules of administrative liability

As no legislation explicitly and exclusively regulates issues related to social media, there is also no unified system of administrative offenses committed online. However, two branches of administrative law have a closer connection to social media platforms or Internet regulation in general.

The first is *personal data protection*, which has a constitutional basis, as the Constitution in Art. 19 (3) states in general that "*everyone has the right to protection against unauthorized collection, disclosure and other misuse of his or her personal data*." The Slovak Act on Personal Data Protection defines personal data in an almost identical wording to that of Art. 4 (1) of the GDPR.[78] It can be stated that there is no substantive difference between the two pieces of legislation regarding the definition of personal data. Slovak regulations do not explicitly contain data management rules for social media providers. Thus, these are also subject to the general rules set out in the GDPR, the content of which has been taken over by the Slovak legal system and virtually unchanged. Pursuant to Section 110 (1) of the Act on Personal Data Protection, *the Office for Personal Data Protection* acts as the

78 Regulation (EU) 2016/679 of the European Parliament and the Council of 27 April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

supervisory authority in the field of data protection. Apart from the courts, there is no other body that can play a meaningful role in data protection in relation to social media.

Slovak courts have dealt with violations in which personal data has become illegally available on the Internet. On several occasions, local governments or other persons in the role of data controllers have been fined by the data protection office, after which the case has been brought to court. An example is decision 1S/243/2017 when the District Court in Bratislava upheld a fine imposed on a municipality by a data protection office because it illegally displayed personal data about affected persons on its own website. In another decision – 6S/96/2019 District Court, the Court annulled a decision of the Office for Personal Data Protection imposing an unusually high penalty (€ 25,000) on an individual who illegally disclosed personal data as an operator of a publicly available directory, which also occurred on its own website. In this case, the court did not refute the infringement itself, but found the fine imposed by the data protection office to be too severe. *Based on the available sources, no court decision specifically addresses data breaches on social media platforms or search engine providers.*[79]

The Office for Personal Data Protection has not issued its own guidelines or other documents addressing the protection of personal data in relation to social media. Only Guidelines 8/2020 on the targeting of social media users,[80] developed by the European Data Protection Board, can be found on the office's website. According to the available sources, the Slovak data protection authority has addressed at least one case of a data breach related to the services of community platforms. In the known case, the data controller (institution providing childcare services) published a photograph of a child on a community platform with the prior consent of the child's legal representative. The legal representative later requested the deletion of the photograph from the social media interface, which was rejected by the data controller, who later argued that the photograph was needed for criminal proceedings. However, in the opinion of the Office for Personal Data Protection, the child's right to data protection in the given case took precedence over the legitimate interests of the data controller. Thus, this constituted a violation of Art. 5 (1) (a) GDPR, adding that the legal basis of the data was subject to display.[81] Furthermore, *if illegal content appears on a website that violates the data protection rules, the Office may oblige the data controller to take* measures to remedy the identified deficiencies (in this case, to delete the illegal content).[82]

Aside from personal data protection, electoral rules contain the soma aspects of political campaigns on social networks. The election campaigns and the order of elections are regulated by Act no.181/2014 on the election campaign. (*zákon č.*

79 See: https://bit.ly/3tBGkWF.
80 See: https://bit.ly/392k7HN.
81 See: https://bit.ly/3Aam9S3.
82 Pursuant to Section 99 of the Act on Personal Data Protection.

181/2014 Zb. o volebnej kampani)[83] and Act no. 180/2014 on the conditions for exercising the right to vote. (*zákon č. 180/2014 Zb. o podmienkach výkonu volebného práva*)[84]. The Ministry of the Interior is responsible for conducting elections; some oversight functions are performed by *the State Committee for the Supervision of Electoral and Political Party Financing*, but ultimately by the Supreme Administrative Court[85] and the Constitutional Court.[86] The Slovak legislation is based on the concept of a closed election campaign,[87]—an election campaign can only be conducted by certain legal entities—so above all by the political parties and their representatives participating in the election; third parties may only participate in an election campaign with prior registration. The active participation of other people in the election campaign is prohibited.

The basic requirement for political advertising during an election campaign is that it is transparent, meaning that the voter can clearly identify the nature of political advertising, which political party has created the advertisement, and the identity of the advertising agency. This restriction also applies to opinion polls.[88] An election campaign can only be conducted during the election campaign period, which lasts until 48 hours before the election announcement, after which there is campaign silence.[89] In addition, political advertising on radio and television may only be broadcast during the period set aside for that purpose—between 21 and 48 hours before the elections[90]—and the results of election polls may no longer be made public from the 14th day before the elections.[91] The law also regulates the timeframes for election advertisements on radio and television. In this context, *freedom of expression can be exercised within significant limits in the context of political advertising.*[92] It is therefore interesting that *the law explicitly excludes its own applicability to online media*, so under § 12 (6) and § 14 (2) of the Act on Election Campaign, the political campaigns restrictions – with the exception of the rules on

83 This legislation contains detailed regulations on election campaigns, such as who can conduct election campaigns and political agitation under what conditions. See: https://bit.ly/394fDAu.

84 This law contains the rules for the conduct of elections, how the right to vote can be exercised, and what operational tasks each state body has in the conduct of elections. See: https://bit.ly/3hvmnMl.

85 Pursuant to Art. 142 (2) of the Constitution, the Supreme Administrative Court decides on the legality and constitutionality of local elections.

86 Pursuant to Art. 129 (2) of the Constitution, the Constitutional Court decides on the legality and constitutionality of the presidential, parliamentary, and European elections.

87 Orosz, 2016, pp. 105–106.

88 Section 15 of the Act on Election Campaign: Everyone who is running an election campaign is obliged to ensure that political advertisements, paid advertisements, published election posters, and all other ways of conducting an election campaign contain information about the customer and producer; the same applies to present pre-election and opinion polls.

89 Section 2(2) of the Act on Election Campaign: The election campaign begins on the day of the publication of the decision to declare the election in the Collection of Laws of the Slovak Republic and ends 48 hours before the day of the election.

90 Section 12 of the Act on Election Campaign.

91 Section 17 of the Act on Election Campaign.

92 There has been a wider academic debate around these limitations. See Orosz, 2016, pp. 105–106.

transparency – do not apply to "transmissions over the internet." Regarding the requirements of the rules and restrictions *on the publication of the results of opinion polls, the law does not contain any provision for internet media*. Restrictions on a certain level of freedom of expression during the election campaign do not concern substantive issues (the Committee or the ministry does not check who said what during the election campaign) but are aimed at complying with formal conditions (e.g., registration obligation, monitoring, breaches of campaign silence, etc.). The Committee may impose a fine of between €1,000 and €300,000 to a political party or a candidate that breaches the campaign silence or discloses the results of a poll.[93] Ultimately, however, the Committee cannot interfere in political communication, so it cannot judge whether a message contained in political advertising violates constitutional and legal restrictions on freedom of expression, provided that political advertising is formally lawful. *The state committee for the supervision of electoral and political party financing has no power to sanction the unauthorized deletion of content on social or other media.*

Further discussions must concern the field of misdemeanors, such as misdemeanors against civil society,[94] among which are offenses committed by a person who *a)* injures the honor of another by insulting or ridiculing him; *b)* intentionally makes a false or incomplete statement to a public authority, a municipal authority, or an organization for the purpose of obtaining an unjustified advantage, and *c)* intentionally disrupts civil coexistence by threatening bodily harm, minor bodily harm, false accusations of misconduct, endorsements, or other abusive behavior. Such unlawful behavior can be fined up to €331. Other types of non-criminal offenses in the online space are represented by misdemeanors of extremism,[95] which can be committed when a person: *a)* uses in public a written, graphic, pictorial, visual, audio, or audio-visual representation of texts and statements, flags, badges, slogans or symbols of groups or movements and their programs or ideologies that are directed towards the suppression of fundamental human rights and freedoms; *b)* uses in public written, graphic, pictorial, visual, audio or visual-sound design advocating, supporting or inciting hatred, violence, or unjustifiably different treatment against a group of persons or an individual because of their membership of a race, nation, nationality, color, ethnic group, descent, or religion. This behavior can be fined up to €500.

Considering the individual administrative branches, unwanted advertisements must also be taken into account. *The freedom of expression includes the right to disseminate information, which has a commercial character* in the interest of the promotion of certain products, which includes the dissemination of such information via the Internet.[96] This is regulated by the provisions of the *e-Services Act* and falls into

93 That is, 48 hours before the election. See: Section 2(2) of the Act on Election Campaign.
94 Section 49 of the Act on Misdemeanors.
95 Section 47a of the Act on Misdemeanors.
96 Jakab, 2016, pp. 171–172.

the category of *unsolicited commercial communications* (which are the main regulations of this act). This is a negative phenomenon for several reasons, mainly due to threats to privacy, customer fraud, and risk to minors and adolescents. In addition, a significant portion of spam has a deceptive or even fraudulent nature, contains pornographic material, unreasonable violence, or incitement to hatred.[97] The problematic act itself, in some parts, falls under the GDPR regulation, but the e-Services Act together with the e-Commerce Directive provide a relatively complex regulation, although this may be subject to change with the planned *Digital Services Act* and *Digital Markets Act.*[98]

7. Closing remarks

Freedom of expression is one of the constitutional cornerstones of a democratic society. The social and technological developments of the last decade made it clear that *the state may not continue to take a passive attitude towards the freedom of speech*, as this is not sufficient to ensure only that the state itself does not intervene in the exchange of information of citizens. Instead, *it must actively guarantee and ensure the realization of freedom of expression and exchange of information*.

Social media is unregulated in Slovakia, and there is currently no legislative intention to regulate it. The scope of the current regulations covers the provision of information society services. Regarding the responsibility of the service provider for content control, the Slovak legislation transposes Art. 14 of the e-Commerce Directive with practically no substantive changes. Thus, under Slovak law, a service provider can be held liable if it has not removed such content after becoming aware of the infringement unless it has produced the content itself or has a significant influence on its production. The service provider has no obligation to monitor the content, and the regulation explicitly prohibits the service provider from searching users' data.

There are no regulations of *the alleged or real censorship of social media platforms*: the main legal doctrine and the Constitutional Court do not define censorship as a phenomenon that can occur between two private entities. *Censorship is only considered an action from the state against freedom of expression,* which some authors consider to be outdated. In this manner, *de facto censorship* differs from *de iure censorship*, which is a narrower term. As a rule, an individual can go to court in the event of the removal of infringing content and an infringement suffered online. In some sectors, such as those concerning the protection of personal data and copyright,

97 Jakab, 2016, pp. 173–174.
98 See: The Digital Services Act package [Online]. Available at: https://bit.ly/3AkREJ6.

there is an administrative supervisory body, including administrative intervention under sectoral legislation.

In the category of "Fake News," the official viewpoint of the Slovak government is that the state must strengthen its own means and capacities for resilience to information operations and cooperate with experts from the public and private sectors to detect and analyze false information. Based on this, a government plan was created (but not yet implemented) to strengthen state reactions to various elements of information operations, reacting primarily to false reports, hoaxes, conspiracy theories, disinformation, and malinformation. Whether such operations can be carried out effectively in accordance with human rights legislation, freedom of speech, unrestricted access to information, and basic human freedoms guaranteed by the Constitution of the Slovak Republic is yet to be seen.

Bibliography

BARTOŇ, M. (2002) *Svoboda projevu a její meze v právu České republiky***,** Praha: Linde, a.s.

Delfi AS v. Estonia, [Online]. Available at: https://bit.ly/3A8wNsL (Accessed: 31 May 2021).

DRGONEC, J. (2015) 'Zákaz cenzúry podľa Ústavy Slovenskej republiky: Implikované základné právo alebo ústavný princíp a súvisiace otázky' *Právník*, 1., pp. 61-79. [Online]. Available at: https://bit.ly/3C2tuUi (Accessed: 31 May 2021).

European Democracy Action Plan [Online]. Available at: https://bit.ly/39iOMRv (Accessed: 31 May 2021).

ĎURAČOVÁ, M. (2005) Translation of the Slovak Criminal Code [Online]. Available at: https://bit.ly/3z79dv8 (Accessed: 31 May 2021).

Európsky parlament žiada jasnú legislatívu pri odstraňovaní obsahu na sociálnych sieťach [Online]. Available at: https://bit.ly/3lnG1uH (Accessed: 31 May 2021).

FILIP, J. (1998) 'Dogmatika svobody projevu z hlediska teorie, legislativy a soudní praxe' *Časopis pro právní vědu a praxi*, Vol. 4, pp. 618–637.

Final results of the Eurobarometer on fake news and online disinformation [Online]. Available at: https://bit.ly/3C7mrtv (Accessed: 31 May 2021).

Guidelines 8/2020 on the targeting of social media users [Online]. Available at: https://bit.ly/3A4c9d4 (Accessed: 31 May 2021).

HUSOVEC, M. (2012) *KS Trenčín: Zodpovednosť poskytovateľa diskusného fóra za údajne difamačné príspevky tretích osob*, [Online]. Available at: https://www.lexforum.sk/405 (Accessed: 31 May 2021).

Information Disorder: Toward an interdisciplinary framework for research and policy making, Council of Europe report DGI(2017)09 [Online]. Available at: https://bit.ly/2X8DSuB (Accessed: 31 May 2021).

KLEIN, T. (2018) 'Az online diskurzusok egyes szabályozási kérdései' in: Klein, T. (eds.) *Tanulmányok a technológia- és cyberjog néhány aktuális kérdéséről*. Budapest: Médiatudományi Intézet. [Online]. Available at: https://nmhh.hu/dokumentum/194190/MK30web.pdf (Accessed: 31 May 2021).

KOLTAY, A. (2019) 'A social media platformok jogi státusa a szólásszabadság nézőpontjából'**,** *In Medias Res.* [Online]. Available at: https://bit.ly/3zazR6d (Accessed: 31 May 2021).

Koľko Slovákov je na sociálnych sieťach? [Online]. Available at: https://bit.ly/3z79wpM (Accessed: 31 May 2021).

Králi sociálnych sietí na Slovensku: Facebook, YouTube a Instagram [Online]. Available at: https://bit.ly/3EobOEO (Accessed: 31 May 2021).

MAJERČÁK, T. (2016) 'Obmedzenie slobody prejavu a práva na informácie v zákone o volebnej kampani' in Majerčák, T. (eds.*) Sloboda prejavu a jej limity – IV. ústavné dni*. Košice: UPJŠ [Online]. Available at: https://www.upjs.sk/public/media/17625/05_SlobodaPrejavu.pdf (Accessed: 31 May 2021).

MORAVEC, O. (2013) *Mediální právo v informační společnosti*, Praha: Leges.

PAVLÍČEK, V. ET AL. (1999) *Ústava a ústavní řád. 2. Díl,* Praha: Linde, a.s.

Nález Ústavného súdu Slovenskej republiky sp. zn. II. ÚS 307/2014 z 18. decembra 2014 [Online]. Available at: https://bit.ly/3C8U2n6 (Accessed: 31 May 2021).

RADOMÍR, J. 'SLOBODA PREJAVU A SPAM' IN MAJERČÁK, T. (eds.*) Sloboda prejavu a jej limity – IV. ústavné dni*. Košice: UPJŠ [Online]. Available at: https://bit.ly/3ntTgwL (Accessed: 31 May 2021).

Orosz, L. (2016) 'Sloboda prejavu vo volebnej kampani' in Majerčák, T. (eds.*) Sloboda prejavu a jej limity – IV. ústavné dni*. Košice: UPJŠ [Online]. Available at: https://www.upjs.sk/public/media/17625/05_SlobodaPrejavu.pdf, (Accessed: 31 May 2021).

Podľa Klusa by mali sociálne siete prijať väčšiu zodpovednosť: Musíme bojovať proti dezinformáciám [Online]. Available at: https://bit.ly/3nv9F3R (Accessed: 31 May 2021).

Programové vyhlásenie Vlády SR [Online]. Available at: https://rokovania.gov.sk/RVL/Material/24756/1 (Accessed: 31 May 2021).

Sociálne siete musia na seba prebrať viac zodpovednosti, zhodli sa Bilčík a Šimečka [Online]. Available at: https://bit.ly/3z8S58e (Accessed: 31 May 2021).

Správa o stave ochrany osobných údajov za obdobie 25. MÁJ 2018 až 24. MÁJ 2019 [Online]. Available at: https://bit.ly/3C6lMZf (Accessed: 31 May 2021).

Správa o stave osobných údajov za rok 2020, Úrad na ochranu osobných údajov Slovenskej republiky [Online]. Available at: https://bit.ly/3tGV1aT (Accessed: 31 May 2021).

Vládny materiál: Koordinovaný mechanizmus odolnosti Slovenskej republiky voči informačným operáciám [Government material: Coordinated mechanism of the Slovak Republic's resilience to information operations] [Online]. Available at: https://bit.ly/3A8TcpL.