First Annual Monitoring and Regulation Report

This project has received funding from the European Union CEF-TC-2020-2. Contract number: 2020-EU-IA-0267

Introduction

This report is part of the CEDMO activity focused on the regulation of disinformation. As a part of this activity, CEDMO monitors and analyzes the current regulatory landscape in the field of media regulation, illegal content, disinformation, and other related topics. This report aims to provide an overview of regulations concerning disinformation and similar concepts in three selected countries - the Czech Republic, Slovakia, and Poland.

The report is divided into twelve sections. Each section covers different regulatory aspects and provides an overview of each country. The report mainly focuses on the existing regulation in all three countries. A few parts of this report cover soft law instruments and proposed policies. In this sense, the goal of this report is not to evaluate the efficiency of the current legal instruments or proposed policies. For this purpose, CEDMO will publish a written recommendation in 2023.

Methods

The report is based on a questionnaire created by EDMO. The first section provides a brief overview of the main findings, describes the main similarities in the legal systems of all three countries, and covers in which aspects the existing regulation departs. The remaining parts cover different aspects of regulatory issues connected to disinformation and similar concepts. Each section covers a topic or an aspect of regulation which stems from the EDMO questionnaire. Since this report aims to provide an overview of how each state approaches challenges posed by disinformation, the prevailing method in this report is description and analysis.

1. Observed Similarities and Differences among the Studied Countries

Based on our findings, none of the three countries recognizes disinformation (or any similar notion) as a legal category. This means that none of the three countries has a legal definition of this concept or any law specifically concerning disinformation. Additionally, none of the countries took any measures against disinformation on a regional level.

All three countries took specific measures after the war in Ukraine. In the Czech Republic and Slovakia, the selected tool to fight disinformation was blocking of certain websites. However, the legal basis significantly differed in both countries, as explained further in this report.

In general, the choice of tools for fighting disinformation differs. For example, Poland prefers educational campaigns. In the Czech Republic, we can see discussions about a new law tackling disinformation if they threaten national security.

Both the Czech Republic and Slovakia attempted to introduce a new crime of spreading disinformation. In both cases, the attempt faced a massive backlash, and as of now, it did not proceed any further.

2. Definitions Used by Policymakers to Define Disinformation, Misinformation, or Related Concepts

a) Czech Republic

There is no official definition in Czech law regarding disinformation or misinformation. However, a few definitions might be found across various policy materials or as a part of documentation published by NGOs specializing in exposing fake news/disinformation.

The Czech Ministry of Interior published a glossary concerning disinformation, misinformation, and propaganda. According to this glossary, **disinformation** is a "*the spreading of deliberately false information, especially by state actors or their offshoots vis-à-vis a foreign state or the media, with the aim to influence the decisions or views of those who receive it*".[1]

This definition differs slightly from the definition provided in the 2018 Code of Practise on Disinformation.[2]

Similarly, **misinformation** is defined as *incorrect or misleading information that is neither systematically nor deliberately disseminated with the intention of influencing the decisions or opinions of those who receive it. Although a neutral phenomenon, misinformation, when spread widely and without proper correction, it may lead to the same result as disinformation - i.e., the adoption of decisions or opinions based on false information."*[3]

The core difference, therefore, lies in the intent of the person who spreads such information.

The Ministry of Interior also recently published their proposal for **a law concerning spreading of content threatening national security.** This proposal does not mention disinformation explicitly, however, it recognizes a category of online information that may threaten national security. The concerned online content is defined as "*online information content that is capable of threatening the sovereignty, territorial integrity and democratic foundations of the Czech Republic or that may significantly endanger the internal order and security of the Czech Republic*".

As mentioned above, various NGO use their own definitions. For example, a website Manipulátoři, focused on uncovering disinformation, uses the following definition: "*lying, deceptive, false information intended to affect the judgement and opinion of an individual, several persons or the whole society.*"[4]

Similarly, another NGO defines a hoax as „*a type of disinformation, in other words, an alarming message that encourages further spreading by its artificial/false/fabricated urgency.*"[5]

b) Slovakia

Same as in the Czech Republic or Poland, Slovak law has no official definition regarding disinformation or misinformation. The term disinformation/misinformation has yet to be codified in

[1] https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

[2] „verifiably false or misleading information" which, cumulatively, (a) „Is created, presented and disseminated for economic gain or to deceive the public intentionally"; and (b) „May cause public harm", intended as „threats to democratic political and policymaking processes as well as public goods such as the protection of EU citizens' health, the environment or security"

[3] https://www.mvcr.cz/chh/clanek/definice-dezinformaci-a-propagandy.aspx

[4] https://manipulatori.cz/lexikon/dezinformace/

[5] https://zvolsi.info/surfarovym-pruvodcem/

the Slovak Republic. Mostly, definitions given in professional publications or official European documents, which are similar and describe the essence, are adopted.

National Security Authority (NBÚ), one of the authorities dealing with the issue of disinformation, has published on its official website the following definition: "*Disinformation refers to false or manipulated information that is disseminated deliberately to mislead and cause harm. Disinformation can take the form of false or manipulated text, images, video or audio and can be used to promote conspiracies, spread doubt and discredit truthful information or individuals and organizations. Even truthful information can be considered disinformation if it is presented in a manipulative manner. Disinformation does not include unintentional errors in reporting, satire, parody, or news and commentary biased in favor of one side that is clearly labeled as such*"[6]

This differs from the widely used definition in the 2022 Strengthened Code of Practice on Disinformation.[7]

On the other hand, misinformation is defined by National Security Authority as "*misleading or false information which, unlike disinformation, is spread unknowingly and without intent to harm*", which is more in line with the definition used in the 2022 Strengthened Code of Practice on Disinformation.

A new initiative from the Ministry of Investments, Regional development and Informatization of the Slovak Republic (MIRRI) introduced a new legislative initiative called *Act on measures to enhance the security and trustworthiness of platforms in the online environment and amending certain laws*.[8] This material defines disinformation as: "*...information that is manifestly false, which is created, presented and disseminated to deceive the public or a certain group of persons and has or may have the effect of causing damage or injury or securing a benefit".* Besides the definition of disinformation, it also proposes a definition of disinformation activity as follows: *"A disinformation activity is the creation, presentation, or dissemination of disinformation".* However, this definition cannot be considered an official definition, but only as an initiative to codify this term.

c) Poland

There is no legal definition of disinformation, misinformation, or any similar concept in Poland. Moreover, no legal act is dedicated to disinformation as a social, political, or legal phenomenon. A trend change was the appointment of Government Representative for the Security of the Information Space of the Republic of Poland by regulation from August 2022 (Dz.U. 2022.1714). However, there is no legal definition of the phenomenon itself.

The Polish legislator and other public entities overwhelmingly use the term *disinformation*. For example, in the Report of the National Broadcasting Council from December 2020[9], the authors

[6] https://www.nbu.gov.sk/urad/o-urade/hybridne-hrozby-a-dezinformacie/dezinformacie/index.html
[7] https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
[8] https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2023-129
[9] https://www.gov.pl/web/krrit/fake-news—dezinformacja-online

reconstruct the definition of disinformation from documents published by other bodies, e.g. the European Parliament (Resolution 2016/2030(INI)), the Council of Europe (Information Disorder: Toward an interdisciplinary framework for research and policy-making), or the output of researchers of the phenomenon. According to the Polish council disinformation is: *"intentional action aimed at causing changes in the awareness of recipients, changes of attitudes towards phenomena and provoke a specific social, economic or political reaction"*[10].

Similarly, authors of many official materials try to stick to the notion of disinformation. Such nomenclature is adopted both in announcements by public authorities (central as well as local government level), in reports of both governmental and state research institutes, and in reports and materials prepared by sectoral organizations and materials prepared by NGOs, as well as in any other widely understood material to which we can attribute the characteristics of a message addressed to a broad audience.

Analysis of the public discourse indicates the use of the interchangeable term disinformation or the polonised term „fejk news" [from English fake news]. However, the use of one or the other depends on the nature of the information, its sender and the addressee. The more a political dispute there is, the more it is possible to use the term fake news.

3. Legislative and Non-Legislative Tools Used in the Studied Countries

a) Czech Republic

Since there is no specific law on disinformation in the Czech Republic and no official definition of this phenomenon, it can be concluded that the non-legislative tools are prevailing.

Legislative tools. The spreading of disinformation may fulfill a definition of certain crimes in the Czech criminal code. The list is provided as a part of section 4 of this report. It must be emphasized that criminal law shall only be applied in cases involving a certain level of social harm. Other legal instruments, such as civil liability, shall apply in other cases. To illustrate this, a defamation claim will most often be pursued according to civil law rather than criminal law.

The issue of disinformation is also connected to freedom of speech. For example, when it comes to personal rights and privacy and media regulation, a body of case law distinguishes between a factual statement and a judgment.

The Czech Ministry of Interior recently prepared a first draft for **a law concerning the spreading of content threatening national security**. This new regulation does not explicitly mention disinformation. However, it is colloquially known as a disinformation regulation, and the media refers to this law as such. The proposal is still in its very early stages and faces criticism because it is seen as a tool for blocking online content.

Non-legislative tools. The non-legislative tools are not primarily state-coordinated. However, recently, the Ministry of Interior, the Ministry of Defence and the Ministry of Justice published "Analysis of the Czech Republic's readiness to face a serious disinformation wave". This Analysis

[10] ibidem, p. 10.

was created based on an Action plan for National Security Audit.[11] This Analysis mostly focuses on disinformation, a mass phenomenon that may threaten a state´s security and sovereignty.

In March 2022, the government also created the position of Government Commissioner for Media and Disinformation. However, this position was canceled in February 2023.

Most of the tools, such as raising awareness or providing fact-checking, thus lie in the hands of NGOs.

There are several NGOs focused on fact-checking in the Czech Republic. For example:

- Demagog
- Manipulátoři
- Čeští elfové
- Kremlin Watch

b) Slovakia

Since there is no specific law on disinformation in Slovakia and no official definition of this phenomenon, it can be concluded that non-legislative tools prevail. Many Slovak NGOs, such as Globsec, Adapt Institute, and Infosecurity, aim to counter disinformation. On the other hand, many state institutions, such as the Council for Media Services, National Security Authority, The Slovak Police Force, Situation Centre of the Slovak Republic are active in this topic.

Legislative tools. One of the newest legislative tools that cope with disinformation is Media Services Act (Act no. 264/2022)[12], which gives new competences to the Council for Media Services, the Slovak national regulatory authority. Specifically:

According to Section 110(3)(g), the competences of the Regulator shall further include: *„initiating and carrying out research and analytical activities in the media field in order to monitor and assess the state of the media environment, in particular concerning the dissemination of hate speech, disinformation, content that may seriously impair the development of minors, cyberbullying, media literacy, media commercial communication, political promotion, internal and external media pluralism and the level of media freedom".*

According to Section 110(3)(q), the Council has competencies to „*cooperate with online platforms for sharing content in the effective, proportionate and non-discriminatory application of the rules for their services*". This is followed by Section 152(8), where „*the content service provider is obliged to provide cooperation to the regulator, especially when carrying out activities according to Section 110(3)(q); for this purpose, he is obliged to provide information upon request and to enable the establishment of access to his service so that the performance of these activities is as efficient as possible.*"

[11] The material can be accessed here: https://www.mvcr.cz/chh/clanek/analyza-pripravenosti-ceske-republiky-celit-zavazne-dezinformacni-vlne.aspx

[12] https://www.slov-lex.sk/pravne-predpisy/SK/ZZ/2022/264/20230101

Besides that, according to Section 153(1) the Regulator has competences to cope with illegal content accordingly:

"If it is proven in the procedure for the prevention of illegal content that the content in question constitutes illegal content and at the same time its dissemination endangers the public interest or constitutes a significant interference with the individual rights or legitimate interests of a person within the scope of the legal order of the Slovak Republic, the regulator shall issue a decision on the prevention of the dissemination of illegal content, by which it shall order the provider of the content sharing platform or the provider of a content service that does not require authorization under this Act to remove the illegal content in question and to prevent its further dissemination."

Definition of illegal content According to Section 151(2):
„For this Act, illegal content is content that:
a) fulfils the characteristics of child pornography or extremist material,
b) incites conduct that fulfils the characteristics of one of the criminal acts of terrorism,
c) approves an action that fulfils the characteristics of one of the criminal acts of terrorism, or
d) fulfils the characteristics of the criminal offense of denying and approving the Holocaust, crimes of political regimes and crimes against humanity, the criminal offense of defaming a nation, race and belief or the criminal offense of inciting national, racial and ethnic hatred."[13]

Non-legislative tools. The non-legislative tools are not primarily state-coordinated. However, in 2022, the Ministry of Defense published the *Action plan for coordinating the fight against hybrid threads 2022-2024.*[14] This document mostly focuses on strengthening state and societal resilience to hybrid threats and strengthening cooperation and coordination for early detection, analysis, attribution and response to hybrid activities against the Slovak Republic.

Most of the tools, such as raising awareness or providing fact-checking, thus lie in the hands of NGOs. There are several NGOs focused on fact-checking in Slovakia, such as Infosecurity.sk, Konspiratori.sk or Demagog.sk. Also, there are activities with a significant impact from Slovak Police Force, which operates the Facebook page called: „Hoaxy a podvody – Polícia SR". The page aims to share information on detected misinformation narratives and raise awareness of online scams.

c) Poland

In Poland's case, both legislative and non-legislative tools can be identified. Nevertheless, due to the general nature of the legal norms contained in the legislation that can be used to deal with disinformation, it should be assumed that non-legislative tools mainly dominate public space and public awareness.

---

[13] Act No. 300/2005, Penal Code, Section 424(1) „*Whoever publicly incites violence or hatred against a group of persons or an individual because of their real or assumed membership of a race, nation, nationality, ethnic group, because of their real or assumed origin, colour, sexual orientation, religion or because they are non-religious, or publicly incites the restriction of their rights and freedoms, shall be punished by imprisonment for up to three years.*"

[14] https://www.nbu.gov.sk/wp-content/uploads/2022/08/AKCNY-PLAN-KOORDINACIE-BOJA-PROTI-HYBRIDNYM-HROZBAM

What does this mean? Laws (i.e. means of dealing with disinformation), no matter whether they contain one or more legal norms (which are abstract and primarily general in nature), are interpreted and applied in the process of law application, both administrative and judicial, to specific factual situations.

Legislative tools. As mentioned in the previous section, as of the date of the report, there are no norms dedicated to specific manifestations of disinformation (information war around the war in Ukraine, the COVID-19 pandemic, etc.) in the Polish legal system. There are legal provisions which, due to their abstract nature, can be applied to the fight against disinformation when properly interpreted (these are discussed in the next sections of this report). The very process of both law-making and its application is reserved for the state. As such, it is impossible in a democratic system based on the Constitution for legal tools to be applied by entities separate from the state.

The provisions sanctioning disinformation activities in a specific context are scattered throughout the legal system. For example, Article 12 para. 1(1) of the Press Law (Journal of Laws 2018.1914) orders the journalist to be diligent and reliable when collecting and using press materials, especially the obligation to falsify the information obtained. Another example of contextual action against disinformation is the obligation to publish almost immediately the rectification of untrue information during the information noise associated with the election campaign. This involves rectifying false claims within the framework of 'election mode'. The obligation to do so derives from Article 111 of the Electoral Code Act (Journal of Laws 2022.1277).

Non-legislative tools. In Poland, non-legislative tools are mostly educational and information programmes, awareness-raising campaigns, both on a direct governmental level (Worth reading - Special Services - Gov.pl Portal www.gov.pl), within centrally financed units (e.g. the National Research Institute NASK - https://cyberpolicy.nask.pl/category/dezinformacja/, or a special team established within the UMCS - https://www.umcs.pl/pl/o-nas,21318.htm), as well as within the execution of their tasks by local governments (information campaigns of municipalities, e.g. Lipsk Municipality, Podlaskie Voivodeship: Municipal Office in Lipsko - Be resistant to disinformation).

4. The Role of Criminal Law

c) Czech Republic

As a preliminary point, it should be emphasized that the Czech criminal code only applies in cases where the perpetrator´s actions are socially harmful and the application of liability according to other legal regulations (such as civil liability) does not suffice.[15] This means that criminal law in general should not be the main instrument for fighting disinformation. Moreover, culpability either in the form of intent or negligence is required to trigger criminal liability.[16]

The Czech criminal code recognizes a few crimes that might be committed while spreading disinformation. However, none of these crimes is specifically intended for disinformation as such. This concerns the following crimes:

[15] Section 12 (2) of the Czech criminal code.
[16] Section 13 (2) of the Czech criminal code.

- Defamation
- Spreading of Alarming News
- Defamation of a Nation, Race or Conviction; Incitement of National and Racial Hatred
- Infringement of Rights of Another
- False Accusation
- Instigation of Hatred towards a Group of People or of Suppression their Rights and Freedoms
- Incitement to Criminal Offence

All the crimes mentioned above require an intent of the perpetrator.

Recently, the Ministry of Interior published that they plan to introduce a proposal to amend the criminal code. This amendment will add a new crime concerning intentional disinformation with potential to harm national security.

b) Slovakia

Slovak criminal code recognises a few crimes that might be committed while spreading disinformation, or the criminal code allows for prosecuting the crimes connected to the dissemination of disinformation, but its application is very difficult. However, none of these crimes is specifically intended for disinformation as such. This concerns the following criminal offences:

- dissemination of an alarmist message[17],
- defamation[18],
- sympathy for a movement to suppress fundamental rights and freedoms[19],
- defamation of nation, race and beliefs[20],
- incitement to national, racial and ethnic hatred[21].

None of the criminal offences listed above has been used in prosecutions for spreading disinformation or misinformation. All the crimes mentioned above require the intent of the perpetrator. Recently, MIRRI introduced a new legislative initiative - *Act on measures to enhance the security and trustworthiness of platforms in the online environment and amend certain laws*.[22]

During the pandemic, there was also an initiative from the Ministry of Justice, to codify the spread of disinformation as a criminal offense as follows: "*Whoever produces or disseminates false information which is capable of causing danger of serious alarm to at least part of the population of a place, endangering the lives or health of people or influencing the population in its decision-making on serious issues of society-wide significance, or commits any other similar act verbally or in writing, by means of an electronic communication service, a sound recording, an audio-visual*

[17] Act No. 300/2005, Penal Code, Section 361
[18] Act No. 300/2005, Penal Code, Section 373
[19] Act No. 300/2005, Penal Code, Section 422
[20] Act No. 300/2005, Penal Code, Section 423
[21] Act No. 300/2005, Penal Code, Section 424
[22] https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2023-129

recording or any other recording, shall be liable to a term of imprisonment of between one and five years".

It was aimed to stop the spreading of disinformation about Covid-19 but the Slovak Parliament did not accept this novelization of the criminal law.

This amendment of Cybersecurity Act (Act No. 69/2018) gave the Slovak National Security Authority the power to block harmful content until 30th September 2022. However, the current law does not include any specific mechanism or procedure for identifying websites spreading problematic content. There was an initiative, to return the competence to block harmful content by the National Security Authority. The Slovak Parliament has not approved the proposed amendment.

c) Poland

There are no provisions in Polish criminal law that, in their content, directly address the issue of punishing disinformation activities. Nevertheless, due to the specificity of legal norms, some provisions could be applied in the context of sanctioning disinformation. However, the substantive criminal clauses in the Polish legal system are not solely in the domain of the Criminal Code but are also found in other statutes.

As far as the Criminal Code itself is concerned, Article 212 contains a crime of defamation. However, this provision is highly abstract. In order to punish the perpetrator, it is necessary to prove, firstly, that he/she publicly disseminated untruths which resulted in humiliation in the eyes of public opinion of a person, a group of persons, an institution, a legal person or an entity of similar status.

Article 216 of the Criminal Code is similarly structured. It concerns public insulting of another person.

An example of criminal law provisions located outside the Criminal code, which addresses the issue of punishment for speaking untruths in the context of the historical memory of the Polish nation, is Article 55 of the Act on the Institute of National Remembrance - Commission for the Prosecution of Crimes against the Polish Nation (Dz.U.2021.177). It speaks of criminal liability for „publicly and contrary to facts denying the crimes referred to in art. 1 pt. 1 of the Act [Nazi, Communist and other crimes]". Such a person would then face a criminal sanction of up to three years imprisonment.

The essence of criminal law is to ensure public order; therefore, every provision, not only those that can be used to combat disinformation, is designed to protect public order.

5. The Role of Regulators in the Fight Against Disinformation

a) Czech Republic

Since there is no law covering the disinformation specifically, there is also no specific regulator which was given powers to deal with them. As of now, the main regulatory bodies include Czech Telecommunication Office, Council for Radio and Television Broadcasting and Ministry of Interior. However, each of these bodies only have limited powers within their agenda.

Czech Telecommunication Office. CTO has the main authority concerning the regulation of the electronic communications market. Regarding disinformation, its powers are limited. In certain cases, CTO may block disinformation websites, however, this may only be done based on specific legal authorization like the recent EU regulation 833/2014.

Council for Radio and Television Broadcasting. The Council is the main regulator in the field of television and radio broadcasting and audiovisual media services on demand and is part of the ERGA group. Its competencies include monitoring the content of broadcasted news. Specifically, the Council supervises whether the broadcasters provide the public with objective and balanced information. However, the competence is mostly limited to ex-post investigation of the content.

Ministry of Interior. The Czech Ministry of Interior operates a Centre for Hybrid Threats which, among other things, deals with the agenda regarding disinformation. As of now, the ministry is preparing a new law that should tackle the spreading of disinformation. However, the ministry does not have any special powers concerning the spread of disinformation itself.

b) Slovakia

Powers given to regulators can be found for example in the Media Services Act (Act No. 264/2022) or in Cybersecurity Act (Act No. 69/2018). Even though these laws do not give powers to regulators specifically aimed at countering disinformation, they can be at least partially applied to this issue.

The main regulatory bodies include the Council for Media Services, the Ministry of Interior and the National Security Authority. However, each of these bodies only has limited powers within their agenda.

Council for media services – the CMS. Generally, CMS, as the Slovak national regulatory authority, operates in the area of state administration, including, in particular, approving and granting authorizations, registrations, licenses, compliance with obligations and imposition of sanctions under the Media Services Act and assessing the appropriateness of measures to protect the public taken by the provider of a video sharing platform.

The CMS also actively participates in developing generally binding legislation in the field of broadcasting, retransmission, the provision of on-demand audiovisual media services and the provision of platforms for sharing content.

The regulator has the authority to initiate and carry out research and analytical activities in the media field to monitor and evaluate the state of the media environment, in particular concerning the dissemination of hate speech, disinformation, and content that may seriously harm the development of minors, cyberbullying, media literacy, commercial media communication, political promotion, internal and external media pluralism and the level of media freedom.

As of August 2022, the CMS cooperates with online platforms for content sharing in the effective, proportionate and non-discriminatory application of the rules governing the provision of their services.

Also, the regulator acts as a supervisory authority for the implementation of the specific measures under Art. 5 of the EU Regulation on addressing the dissemination of terrorist content online and imposes sanctions under Art. 18 of the same regulation for breaches of the obligations defined by the Media Services Act, as well as sanctions under other specified special regulations.

Ministry of Interior. The Slovak Ministry of Interior operates the **Center for Countering Hybrid Threats**, which, among other things, deals with the agenda regarding disinformation. The ministry does not have any special powers concerning the spread of disinformation itself, but it publishes analytical reports.

The National Security Authority. The National Security Authority covers many activities including the fight against hybrid threats and disinformation. This builds on both National and European efforts. The role of the National Security Authority is to systematically monitor, evaluate, analyze and respond to activities that have the potential to polarize society, introduce insecurity, and thus undermine the legitimacy, and credibility of state institutions and the democratic constitutional order, and thus have a negative impact on the realization of the security interests of the Slovak Republic.

The National Cyber Security Centre SK-CERT, as well as other services of the National Security Authority, cooperate closely in the fight against disinformation and hybrid threats. They provide their outputs to the Situation Centre of the Slovak Republic, which operates at the Office of the Government of the Slovak Republic, and to the National Security Analysis Centre, which is an analytical, communication and cooperation workplace of the Slovak Information Service based on the active participation of Slovak security authorities.

c) Poland

Apart from the Plenipotentiary for Information Space Security, established in September 2022 and described in the previous parts of this report, no regulatory body is dedicated to coordinating policies against disinformation. It should be assumed that, depending on the own initiative of individual constitutional or other state bodies, it is possible to take action against external or internal disinformation policies, but based on already existing legislation.

An example of such an initiative based on already existing legal regulations, but stimulated by specific political events, may be the decision of the National Broadcasting Council to block the broadcasting on the territory of the Republic of Poland of Russian and Belarusian media distributing the Kremlin's propaganda message.[23] In other words, in the aforementioned case, the change in the political environment forced the appropriate application of the law by a body that already had specific powers. In this case, the ability to decide which media can and cannot broadcast in Poland.

Additionally, the actions of the National Broadcasting Council were the implementation of European law - Regulation 2022/350.[24]

[23] https://www.gov.pl/web/krrit/krrit-weryfikuje-wszystkie-wpisane-do-rejestru-rosyjskie-i-bialoruskie-programy-telewizyjne

[24] Council Regulation (EU) 2022/350 of 1 March 2022 amending Regulation (EU) No 833/2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine

6. Policies Regarding Political Advertising on Online Platforms

a) Czech Republic

Political parties and their activity are mainly regulated by the Czech law on political parties and political movements[25] and by the various electoral laws. Although the law covers political advertising and financing, it does contain only a few norms regarding political advertising on online platforms. None of these however deals with targeting or micro-targeting.

The existing laws concern mostly the transparency of advertising. For example, any advertisement must contain information about the sponsor and processor of the advertisement. Similarly, a political party cannot use the social media of the municipality/region for the purpose of a campaign.

b) Slovakia

Political parties and their activity are mainly regulated by the Slovak Act No. 181/2014 on election campaigning. This law, however, does not clearly define whether the regulation also applies to websites and online activities. While the current law requires politicians and political parties to label any paid political advertising in the online environment as part of the election campaign, the proposal for the EU Regulation on the transparency and targeting of political advertising requires the publication of such announcements outside the election period.

c) Poland

There is no official government statement regarding online political advertising. As far as the state agenda is concerned, there has not been any official campaign to tackle or raise public awareness of the dangers of such practices.

The situation is different when it comes to the non-governmental sector. In this case, organizations whose statutory objective is to expose this type of practice do take educational measures. For example, there is a report of the „Panopticon“ Foundation entitled „Who (really) tracked you“.[26] This report states in their recommendations for legal reforms regarding political microtargeting in Polish cyberspace that users still have not received a level of protection corresponding to the minimum requirements introduced by GDPR. The report also shows that microtargeting was not a key issue in the 2019 election campaign.

[25] zákon o sdružování v politických stranách a v politických hnutích

[26] https://panoptykon.org/ktocienamierzyl-raport.

7. Measures Tackling Disinformation on a Regional Level

Czech Republic

There are no specific measures taken on a regional or local level in the Czech Republic.

Slovakia

No specific measures are taken on a regional or local level in the Slovak Republic.

Poland

No specific measures are taken on a regional or local level in Poland. Local self-government and local government units implement state policy. They are its executors and do not demonstrate their own initiatives.

8. Specific Regulations Regarding Disinformation during the Covid-19 Pandemic

a) Czech Republic

No hard-law legal tools were introduced in connection to the COVID-19 pandemic. However, existing legal measures applied in some cases where disinformation was intentionally spread. For example, one person is currently being investigated for committing the crime of spreading alarming news.[27] The person is accused of spreading disinformation through video in which the perpetrator claimed several people died after being vaccinated. At the same time, the person was already ordered to pay damages for spreading this disinformation.

b) Slovakia

The Slovak government and NGOs repeatedly emphasized that public education is the most important task. At the time of the Covid-19 pandemic, awareness campaigns were launched in Slovakia. The campaigns aimed at self-isolation, higher hygiene habits and wearing masks. The second campaign was aimed at Covid-19 vaccination. Furthermore, NGOs such as Infosecurity.sk, Demagog.sk as well as Slovak Police Force and the Ministry of Health of the Slovak Republic started to fact-check the disinformation narratives about Covid-19 and vaccination.

There was also an initiative from the Ministry of Justice, to codify the spread of disinformation as a criminal offense as follows: "*Whoever produces or disseminates false information which is capable of causing danger of serious alarm to at least part of the population of a place, endangering the lives or health of people or influencing the population in its decision-making on serious issues of society-wide significance, or commits any other similar act verbally or in writing, by means of an electronic communication service, a sound recording, an audio-visual recording or any other recording, shall be liable to a term of imprisonment of between one and five years*".

It was aimed to stop the dissemination of disinformation about Covid-19 but this novelization of the criminal law did not pass the legislative procedure in the Slovak Parliament.

[27] https://www.irozhlas.cz/zpravy-domov/jana-peterkova-soud-dezinformace_2301101001_ako

c) Poland

Through its ministers, the Polish government repeatedly stressed that public education, not coercion, was the most important issue. This meant that there was a heavy reliance on mass educational campaigns (e.g. celebrities encouraging self-isolation and vaccination). Separate actions were, in turn, taken by the self-governing bodies of the public trust professions, which stigmatized the unethical attitudes of some doctors.

Additionally, there was one case of a doctor supporting anti-vaccine movements who was banned from practicing his profession.[28] The spreading of statements undermining the necessity of vaccination has been considered by the disciplinary bodies of the medical self-government as violating the Code of Medical Ethics. In other words, once again concepts have been adapted for the interpretation of existing legislation.

9. Specific Regulations Regarding Disinformation in the Context of War in Ukraine

a) Czech Republic

In relation to the war in Ukraine, several websites were blocked in the Czech Republic by the Czech domain registry (CZ.NIC) and a few others by the operators. None of these actions were based on a proper legal basis which resulted in multiple lawsuits against the Czech Republic and the Czech domain registry. Moreover, the only legal documents published by the government were recommendations for the operators to take actions which were vaguely formulated and cannot be considered a suitable legal basis for the action of blocking of the website.

One of the lawsuits was already dismissed by the Supreme Administrative Court. In this particular case, the Czech government was sued. The court ruled that the government cannot be held liable, because they only published a recommendation, not a mandatory legal act. The court also concluded that the freedom of speech was not threatened because only limited number of websites were blocked.

b) Slovakia

The Cybersecurity Act (Act no. 69/2018) was amended in reaction to the war. This amendment gave the Slovak National Security Authority the authority to block harmful content until 30th September 2022. However, the current law does not include any specific mechanism or procedure for identifying websites spreading problematic content. There was an initiative to return the competence to block harmful content to the National Security Authority. The Slovak Parliament has not approved the proposed amendment.

[28] https://www.newsweek.pl/polska/lekarz-antyszczepionkowcow-hubert-czerniak-pozbawiony-prawa-do-wykonywania-zawodu/81cyj56.

c) Poland

In relation to the war in Ukraine, further measures were taken to restrict access to Russian and Belarusian media. All Russian and Belarusian television channels have been removed from cable and satellite television listings. These were mainly news channels and basic state television channels. However, all channels broadcast from Russia and Belarus were considered to be controlled by their respective governments. However, this was an ad hoc action based on legal norms already in circulation (Broadcasting Law)[29], not a dedicated action.

The Polish government also focused on the education of the public, i.e. an attempt was made to reach the broadest possible audience with a counter-dissemination message using all possible channels. Hence, reports and analyses by disinformation research centers were carried out or even reached for warning tools in addition to the usual announcements. This was the case after the Russian shelling of Kramatorsk station in April this year. Text messages were sent to everyone in the area informing them of the disinformation activities of the Russians.[30]

10. The Impact of Code of Practise on Disinformation the Studied Countries

a) Czech Republic

At present, it is not possible to make a reliable assessment of the Code's impact on the policy system to combat disinformation in the Czech Republic. It is also unclear how the definition proposed in the glossary provided by the Ministry of Inferior was influenced by the Code since the definitions are slightly different.

b) Slovakia

It is difficult to determine the Code's impact on the policy system to combat disinformation in Slovakia.

c) Poland

At present, it is not possible to assess the Code's impact on the policy system to combat disinformation in Poland. Information about the Code is residual, limited to communicating that it was created and its objectives. Both governmental websites and units specializing in disinformation research (NASK) have made relevant materials available. Nevertheless, it is difficult to speak of common knowledge of the existence of the Code in the Polish public and information space.

As part of their tasks under the Code, individual corporations with an inter- or transnational reach have announced their adherence to the policy of combating disinformation, e.g. Orange - How to deal with disinformation? [PRACTICAL TIPS] - Orange Foundation.

[29] Polskie prawo medialne - Krajowa Rada Radiofonii i Telewizji - Portal Gov.pl (www.gov.pl)

[30] https://www.polsatnews.pl/wiadomosc/2022-04-26/rcb-ostrzega-przed-dezinformacja-w-sprawie-kramatorska/

11. Measures Aimed at Strengthening the Fact-checking Capacities and Capabilities of Independent Fact-checking Organizations, Media, and Journalists

a) Czech Republic

The main fact-checking activities are provided by Czech NGOs.

There is a manual created by the Ministry of Interior containing steps to verify the information and recognize disinformation.[31]

b) Slovakia

One of the key measures is the creation of a fact-checking portal, Demagog.sk. It is an NGO that evaluates the accuracy of statements made by politicians and public figures in Slovakia and provides readers with reliable and factual information.

In addition, there is the Slovak Press Council, which serves as a self-regulatory body for the Slovak media industry. The Press Council is responsible for promoting ethical journalism standards and addressing complaints related to media content.

The Investigative Centre of Jan Kuciak conducts investigative reporting and provides training and support for journalists in Slovakia.

A good example of fact-checking activity implemented in Slovakia is the page „Hoaxy a podvody – Polícia SR“. Slovak Police Force manages this Facebook page and aims to prevent the negative impact of disinformation by debunking and pre-bunking the most popular and most harmful disinformation narratives in Slovakia. Also, the CEDMO with the fact-check project[32] serves as an example of good practice.

Although, there is still room for improvement, and continued support and investment in fact-checking initiatives are necessary to combat disinformation and promote the accuracy of the information in the Slovak media landscape.

c) Poland

As mentioned in a previous paragraph, the current fight against disinformation in Poland is profiled in the fight against internal threats. At the same time, given Poland's steady decline in all rankings of media freedom and in the face of justified accusations against the authorities for instrumental use of the public media, the credibility of the verification of individual information may raise serious doubts. There are several constitutional and statutory guarantees of freedom of speech and, consequently, of the media. Nevertheless, the level of public trust in the transfer of information is systematically declining.

Specific legal guarantees allow the pursuit of the truth. Nevertheless, the practice of media policy, especially internal media policy, means that the public perception of particular initiatives may be quite the opposite of that expected under a system of constitutional liberal democracy. Currently,

[31] https://www.mvcr.cz/chh/clanek/ke-stazeni-resist-prirucka-pro-boj-s-dezinformacemi.aspx)

[32] https://cedmohub.eu/sk/?_gl=1%2Asovsn3%2A_up%2AMQ..%2A_ga%2AMjA2MzE0NTIwLjE2NzkwNTc3NzA.%2A_ga_1FB9CRHWST%2AMTY3OTA1Nzc2OS4xLjAuMTY3OTA1Nzc2OS4wLjAuMA

in Poland, there is a regression of political initiatives in favor of free media (especially public media) rather than a flourishing of freedom of speech and media independence. The source of this situation is a crisis of the rule of law.

12. Nationwide Data in Connection with the Disinformation Phenomenon

a) Czech Republic

There is a data journalistic project **Česko v datech** which published data on disinformation. They can be accessed via https://www.ceskovdatech.cz/clanek/176-dezinformace/

b) Slovakia

Even though there is no complete, cross-sectional, quantitative data summarizing the phenomenon of disinformation in Slovakia, there are three open databases from NGOs that publish information connected to the disinformation phenomenon.

Konšpirátori.sk – a public database of websites with non-serious, misleading, deceptive, fraudulent, conspiratorial or propagandistic content.

Blbec.online – a public webpage that aims to collect and process publicly available data from Facebook. It already has nearly 530 Facebook pages in its database that spread, for example, fascist posts and misinformation.

Gerulata.com - Gerulata Technologies is a technology company based in Bratislava, Slovakia. It specializes in developing software for STRATCOM and OSINT professionals. This company also published a list of Pro-russian sources in Slovakia.[33]

c) Poland

There are no complete, cross-sectional, quantitative data summarizing the phenomenon of disinformation on the territory of Poland. Nevertheless, individual governmental bodies, state-funded research units, and the non-governmental sector publish reports on disinformation activities online with varying intensity. Examples:

Government report „Disinformation through the eyes of Poles“[34]

NASK report[35]

Reports by the Centre for Propaganda Analysis[36]

[33] https://www.gerulata.com/docs/gerulata_top_pro_russian_sources.pdf?ref=gerulata-technologies

[34] https://www.gov.pl/web/krrit/dezinformacja-oczami-polakow—raport-digital-poland)

[35] https://www.nask.pl/pl/raporty/raporty/2592,Bezpieczne-wybory-raport-na-temat-dezinformacji-w-internecie.html

[36] https://capd.pl/pl/raporty

Conclusion

This is the first report published by CEDMO on regulation overview.

Experience from Slovakia shows us that it is very difficult to come up with a precise legal definition of disinformation. Experience from Poland shows us that well-intentioned regulation promoting freedom of speech could end up as a tool for online censorship. And the experience from the Czech Republic shows us how problematic it is to find a balance in blocking disinformation websites. Questions, such as whether we should block an entire website or only some of its content, arise.

It is also apparent that the states take their actions based on a political situation. For this reason, a certain shift toward the need for disinformation regulation began to appear right after the war in Ukraine started.

CEDMO will further monitor the current legislative tendencies as well as the development in the field of non-legislative tools.

This project has received funding from the European Union CEF-TC-2020-2. Contract number: 2020-EU-IA-0267