АКТУАЛЬНІ ПРОБЛЕМИ РОЗВИТКУ СУЧАСНОЇ МЕДІАСФЕРИ

Медіафорум : аналітика, прогнози, інформаційний менеджмент : зб. наук. праць. – Чернівці : Чернівецький нац. ун-т, 2023. – Том 13. – С. 143-160

Mediarorum: Analytics, Forecasts, Information Management: Collection of Research Articles. – Chernivtsi: Chernivtsi National University, 2023. – Vol. 13. – pp. 143-160

https://doi.org/10.31861/mediaforum.2023.13.143-160
УДК: 341.171:[316.774:004.738.5]

© *Joanna Kulesza*[1]
© *Pavlo Burdiak*[2]

COUNTERING DISINFORMATION ON SOCIAL MEDIA PLATFORMS: DEVELOPMENTS IN THE EU AND POLAND*

One of the biggest challenges to European democracies is the spread of malicious disinformation, facilitated by the increasing importance of online platforms as news sources. The present article sheds light on the initiatives to combat disinformation on social media platforms in the EU. Some insights from Poland are also drawn.

The research reveals that the EU's anti-disinformation activities can be traced back to 2015, which marked the establishment of the East StratCom Task Force, disinformation monitoring project EUvsDisinfo, and Hybrid Fusion Cell. Building on these initiatives, the EU prompted the development of a groundbreaking self-regulatory Code of Practice on Disinformation, followed up and complemented by the legally binding DSA. Both documents provide due diligence standards and promote best practices for combating disinformation on platforms.

With regard to the developments in Poland, notwithstanding some legislative proposals the country lacks comprehensive national policies to address

[1] Director of the Lodz Cyber Hub and assistant professor (tenured) at the Department of Public International Law and International Relations of the Faculty of Law and Administration of the University of Lodz (Lodz, Poland). Email: joanna_kulesza@wpia.uni.lodz.pl; https://orcid.org/0000-0003-0390-6062.

[2] PhD student at the Doctoral School of Law and Political Sciences of the University of Szeged (Szeged, Hungary), visiting researcher at the Lodz Cyber Hub of the University of Lodz (Lodz, Poland) within the Visegrad Scholarship Program. Email: pavloburdiak@gmail.com; https://orcid.org/0009-0007-0319-5412.

* The present article was written by the authors with the support of the International Visegrad Fund.

platform disinformation. It persists as a critical concern, exacerbated by the rule of law challenges since 2015.

The article recommends complementing well-elaborated legal frameworks with media literacy initiatives, civil society engagement, and technological innovations to detect and counter disinformation more efficiently. Such a holistic approach can enhance society's resilience against disinformation while upholding democratic principles and freedom of expression in the digital age.

Keywords: *disinformation, freedom of expression, due diligence, social media platforms, Code of Practice on Disinformation, DSA, EU, Poland.*

Протидія дезінформації в соціальних мережах: досвід ЄС та Польщі

Поширення зловмисної дезінформації у соцмережах є одним із найбільших викликів для європейських демократій. Мета статті – дослідити ініціативи та нормативно-правові інструменти регулювання дезінформації у соціальних мережах, розроблені в ЄС та Польщі. Для досягнення вказаної мети вирішено два завдання. По-перше, проаналізовано нормативно-правову базу ЄС для боротьби з дезінформацією в соцмережах, зокрема Кодекс практики щодо дезінформації та Закон про цифрові послуги. По-друге, висвітлено ініціативи з протидії дезінформації в Польщі, зокрема законопроєкт про захист свобод користувачів соціальних мереж.

Виявлено, що ЄС розпочав активну кампанію з протидії дезінформації у 2015 році. Тоді було створено окрему Оперативну робочу групу зі стратегічних комунікацій, проєкт моніторингу дезінформації EUvsDisinfo і Hybrid Fusion Cell. Крім того, Європейський Союз сприяв розробці новаторської ініціативи саморегулювання онлайн-платформ - Кодексу практики з дезінформації. Положення Кодексу набули більшої ваги після прийняття юридично зобов'язувального Закону про цифрові послуги, який містить безпосередню відсилку до Кодексу. Обидва документи закріплюють стандарти належної обачності та заохочують найкращі практики боротьби з дезінформацією на онлайн-платформах.

З'ясовано, що попри деякі законодавчі ініціативи в Польщі немає комплексної національної політики щодо боротьби з дезінформацією на онлайн-платформах. Ситуація далі ускладнюється через проблеми з верховенством права, що загострилися у країні з 2015 року.

Для ефективного виявлення та протидії дезінформації в соцмережах запропоновано низку рекомендацій, а саме: поєднувати детально розроблену законодавчу базу щодо протидії дезінформації з проєктами медіаграмотності, залученням громадянського суспільства та технологічними інноваціями. Такий комплексний підхід сприятиме підвищенню стійкості суспільства до дезінформації з урахуванням принципів демократії та свободи вираження поглядів у цифрову епоху.

Ключові слова: *дезінформація, свобода вираження поглядів, належна обачність, соціальні мережі, Кодекс практики щодо дезінформації, Закон про цифрові послуги, ЄС, Польща.*

Formulation of the scientific problem and its significance. The battle against disinformation poses a persistent challenge for European democracies and societies. Disinformation erodes citizens' trust in democracy and its institutions while fueling public opinion polarization and interfering with democratic decision-making processes (European Commission and High Representative, 2018).

The rapid development of ICTs and AI, and the growing role of social media platforms not just as a means of communication but also as a news source, have exacerbated the challenges brought about by disinformation. Social media platforms have turned into means for disseminating falsehoods and half-truths. Bots (automated software) and trolls (users who intentionally instigate conflict) may flood social media with harmful disinformation. Posts containing disinformation might go viral. It becomes increasingly complicated to identify manipulated content and deepfakes. The list can go on.

As reported by the EU Hybrid Fusion Cell, disinformation disseminated by the Russian Federation emerges as the most significant threat to the European Union (European Commission and High Representative, 2018). Characterized by its systematic nature, ample resources, active use of social media platforms, and scale surpassing that of other nations, Russian disinformation campaigns pose a formidable challenge to the EU's information landscape. Russia generally steps up its disinformation efforts against the European Union during pivotal events such as elections, both at the level of the EU and Member States; referenda, such as the UK's vote on EU membership; demonstrations, e.g., protests in Catalonia and the Yellow vests movement in France, etc. (Legucka, 2019). Kremlin's goal is

"to sow fear, discord, and paralysis that undermines democratic institutions and weakens critical Western alliances such as NATO and the EU" (Commission on Security and Cooperation in Europe, 2017).

An increased focus of Russian disinformation campaigns is placed on Ukraine. The EU's disinformation monitoring project EUvsDisinfo reported that the prevalence of disinformation cases targeting Ukraine constituted over 40% of all cases documented in their database (EUvsDisinfo, n.d. b.). The Kremlin's active disinformation attacks against Ukraine date back to at least 2014 (the beginning of Russian aggression against Ukraine), but they have intensified following the 2022 full-scale invasion. A fair share of these disinformation campaigns were conducted online, mainly on social media platforms (Legucka, 2019).

Taking into account the threats to democracy and society posed by disinformation and considering the extensive use of social media platforms for spreading harmful falsehoods, it is essential to examine the EU's response to these challenges. The present article focuses on the legal developments within the EU and Poland aimed at countering disinformation on social media platforms.

Analysis of recent research on this problem. In recent years, the issue of regulating disinformation on online platforms has gained prominence in scholarly literature. Alexander Peukert provided an overview of the initiatives aimed at regulating disinformation within the EU (Peukert, 2023). European Digital Media Observatory presented a report assessing the implementation of the Code of practice on disinformation (European Digital Media Observatory, 2020). Agnieszka Legucka shed light on the EU's approach to countering Russian disinformation (Legucka, 2019). Xawery Konarski examined the legal measures to combat online disinformation in the EU and Poland (Konarski, 2022). Mateusz Zadroga and Magdalena Wilczyńska prepared a report on the disinformation landscape and policies to combat disinformation in Poland (Zadroga and Wilczyńska, 2023).

Formulation of the purpose, objectives, and methods of the article. The purpose of the present article is to shed light on the legal development in the EU and Poland aimed at regulating disinformation on social media platforms.

The stated purpose requires attaining two objectives. Firstly, to analyze the EU's legal framework for combating disinformation on platforms, including the Code of Practice on Disinformation and the Digital Services Act. Secondly, to discuss initiatives for countering disinformation in Po-

land, particularly the draft law on "protecting the freedoms of social media users".

To fulfill the outlined objectives, the article employs a blend of methods, including analytical, functional, and descriptive methods of legal research.

Presentation of the main material. Inauguration of the EU's disinformation defense: East StratCom Task Force, EUvsDisinfo, Hybrid Fusion Cell. The EU has been actively developing means for countering disinformation since 2015. At the time, the European Council emphasized the need to counter Russia's ongoing disinformation campaigns and called for the High Representative of the Union for Foreign Affairs, in cooperation with Member States and the EU institutions, to create an action plan and set up a communications team to address Russian disinformation (European Council, 2015). This led to the establishment of the East StratCom Task Force within the Strategic Communications and Information Analysis Division (AFFGEN.7) of the European External Action Service. The East StratCom Task Force's primary responsibilities are to scrutinize disinformation trends, elucidate and unveil disinformation narratives, and heighten awareness of the detrimental effects of disinformation promoted by pro-Kremlin sources in the information space of the EU, Eastern Neighbourhood countries and beyond (European External Action Service, 2021).

The flagship program of the Task Force is EUvsDisinfo. Founded in 2015, it aims to mitigate and respond to the continuous disinformation campaigns perpetrated by the Russian Federation, which significantly impact the European Union, its Member States, and neighboring nations. At the heart of EUvsDisinfo's mission lies the pivotal goal of enhancing public comprehension of Kremlin-led disinformation operations, particularly on social media platforms. It strives to empower citizens in Europe and other regions with the tools to build resilience against manipulation and disinformation in the digital realm (EUvsDisinfo, n.d. a.).

To complement the activities of the East StratCom Task Force, in 2016 the EU Commission and the High Representative of the Union for Foreign Affairs and Security Policy jointly communicated the proposal to create the Hybrid Fusion Cell within the European External Action Service, designed to serve as a centralized hub for the comprehensive analysis of hybrid threats. While the definitions of hybrid threats may vary and need to maintain flexibility to adapt to their dynamic nature, hybrid threats are generally characterized by a combination of coercive and subversive ac-

tivities, employing both conventional and unconventional methods, which may involve the proliferation of disinformation. As stipulated in the joint communication, hybrid threats may manifest through extensive disinformation campaigns, utilizing social media platforms to manipulate the political narrative or to radicalize, recruit, and direct proxy actors, thereby serving as effective vehicles for executing hybrid strategies (European Commission and High Representative, 2016). To respond to these threats, the EU Hybrid Fusion Cell started to provide strategic analysis to the EU decision-makers (European Commission, 2019).

Advancing disinformation policies: from High-level expert group to Code of Practice on Disinformation. The next stage in the development of disinformation policies within the EU took place in January 2018, when the EU Commission established a high-level group of experts ("the HLEG") to provide counsel on policy initiatives aimed at countering the proliferation of fake news and disinformation across traditional media and social media. In March 2018, the HLEG produced a report emphasizing that the rise of digital media and online platforms enabled new forms of disinformation on a larger scale. The report suggested establishing a multistakeholder Coalition (consisting of online platforms, news media organizations, journalists, publishers, independent content creators, fact-checkers, and other practitioners) tasked with designing the self-regulatory Code of Practice for tackling disinformation on platforms (High level Group on fake news and online disinformation, 2018). The same stance was reiterated a month later in a Communication from the European Commission titled "Tackling online disinformation: a European Approach" (European Commission, 2018). Furthermore, both the HLEG report and the Commission Communication put forward a number of guiding principles for developing the Code of Practice to tackle disinformation on platforms, including, but not limited to, the following:

- Platforms should improve their advertising policies and reduce revenues for purveyors of disinformation;
- Platforms should ensure transparency about sponsored content and appropriately distinguish sponsored political advertising from other content;
- Platforms should improve the visibility of reliable and trustworthy content, etc.

The activities of the HLEG and the Commission culminated in the creation and adoption of the voluntary EU Code of Practice on Disin-

formation, which established 21 commitments for platforms in different domains, from transparency in political advertising to demonetization of purveyors of disinformation. It was initially signed in October 2018 by the online platforms Facebook (the company changed its name to Meta in 2021), Twitter (subsequently withdrew in May 2023), Google, and Mozilla. Microsoft signed the Code in May 2019, while TikTok acceded in June 2020. Advertisers and other players in the advertising industry also joined the Code (EU Code of Practice on Disinformation, 2018).

The 2018 Code of Practice on Disinformation was a pioneering initiative, the first one of its kind worldwide, in which the representatives of online platforms, prominent tech companies, and key players in the advertising industry collectively embraced and endorsed voluntary self-regulatory standards to combat the dissemination of disinformation.

The Code was "stress tested" during the COVID-19 infodemic (Peukert, 2023). The 2020 EU Commission's report showed that the Code proved a valuable instrument for ensuring greater transparency and accountability of platforms' policies on limiting disinformation in times of COVID-19 and enhancing the visibility of COVID-19 information disseminated by the World Health Organization and national health organizations (European Commission, 2020a). At the same time, the Commission's overall assessment revealed some structural weaknesses in the Code, ambiguous definitions, and a lack of monitoring and enforcement mechanisms (European Commission, 2020b). Consequently, in May 2021, the Commission took a proactive stance and issued the Guidance on Strengthening the 2018 Code of Practice on Disinformation. The Guidance was meant to serve as a reference point on how the signatories should address the identified shortcomings to enhance the effectiveness and reliability of the Code. The critical areas for reinforcement of the Code were identified as follows (European Commission, 2021):

- larger participation with tailored commitments;
- improved demonetization of disinformation;
- enhanced integrity of services;
- increased empowerment of users;
- expanded fact-checking;
- greater access to data for researchers;
- a more robust monitoring framework.

The revision process for the Code was initiated in June 2021, and the updated Code was presented a year later, in June 2022. It is essential to note

that the 2022 Code of Practice is an outcome of the collaborative efforts undertaken by the signatories. The decision regarding which (if any) commitments to endorse rests with the signatories themselves, and they bear the responsibility for ensuring the effective implementation of their commitments. The Commission did not (and was not supposed to) formally endorse the Code. However, it articulated its expectations in the Guidance and deemed the Code to meet them (European Commission, 2022).

The strengthened Code of Practice on Disinformation interprets disinformation in accordance with the definition offered in the European democracy action plan (European Commission, 2020c). More specifically, it states that the concept of disinformation encompasses the following phenomena (The Strengthened Code of Practice on Disinformation, 2022):

- misinformation - false or misleading content shared without harmful intent though the effects can still be harmful, e.g., when people share false information with friends and family in good faith;
- disinformation - false or misleading content that is spread with an intention to deceive or secure economic or political gain and which may cause public harm;
- information influence operation - coordinated efforts by either domestic or foreign actors to influence a target audience using a range of deceptive means, including suppressing independent information sources in combination with disinformation;
- foreign interference in the information space (often carried out as part of a broader hybrid operation) - coercive and deceptive efforts to disrupt the free formation and expression of individuals' political will by a foreign state actor or its agents.

It is important to note that the concept of "Disinformation" under the Code does not include misleading advertising, reporting errors, satire and parody, or content that is clearly identified as partisan news and commentary.

To fight against the phenomena of disinformation, the strengthened Code suggests 44 commitments and 128 specific measures in the following areas (The Strengthened Code of Practice on Disinformation, 2022):

- demonetization of disinformation: implementing measures to prevent purveyors of disinformation from profiting through advertising revenues;
- increased transparency of political advertising: more efficient labeling of political ads, revealing the sponsor, ad spend, and display period;

- greater integrity of services: countering manipulative behaviors used to disseminate disinformation, such as fake accounts, amplification through bot-driven activities, impersonation, and the malicious use of deep fakes;
- user empowerment: improving tools for recognizing and flagging disinformation, promoting access to authoritative sources, launching media literacy initiatives, etc.;
- researcher empowerment: providing researchers with access to non-personal, anonymised, aggregated or manifestly made public platforms' data to conduct research on disinformation;
- collaboration with fact-checkers: ensuring more active collaboration with fact-checkers regarding the disinformation disseminated on platforms;
- establishment of the Transparency centre*: providing a comprehensive overview of the implementation of the Code's measures in the Transparency centre;
- establishment of the Task-force: ensuring that the Code remains current and fit for purpose by creating the Task-force to review and adjust the Code in light of ongoing developments in technology, society, markets, and legislation;
- improved monitoring framework: elaborating special Service Level Indicators to measure the Code's implementation.

The preamble of the Code indicates that its provisions are designed to complement regulatory requirements and objectives set out in the Digital Services Act (DSA), Article 45 of which encourages the drawing up of voluntary codes of conduct to tackle different types of illegal content and systemic risks (European Parliament and Council of the EU, 2022).

Disinformation regulatory landscape in the EU under the Digital Services Act. The Digital Services Act arguably stands as the most significant and ambitious legally binding regulation worldwide in terms of safeguarding the digital space against the proliferation of illegal and harmful content, including disinformation, while upholding users' fundamental rights. Its scope extends to regulating various online intermediaries and platforms (European Commission, 2023), encompassing social media platforms (e.g. very large online platforms like Facebook, Instagram, LinkedIn, Pinterest, Snapchat, TikTok, Twitter, YouTube), online marketplaces (e.g. Alibaba

* https://disinfocode.eu/

AliExpress, Google Shopping), app stores (e.g., Apple AppStore, Google Play), online travel platforms, (e.g., Google Maps), accommodation platforms (e.g., Booking.com), and search engines (e.g., very large online search engines like Bing, Google Search).

Notably, the DSA provisions are designed asymmetrically, imposing more rigid requirements on very large online platforms (VLOPs) and very large online search engines (VLOSEs), as they have a considerably higher impact on society compared to smaller platforms and search engines. For the VLOPs (including large social media platforms) and VLOSEs the DSA rules became effective as of August 25, 2023. As for other platforms and search engines, they will be subject to the DSA starting from February 17, 2024.

The DSA's objective is to create "a safe, predictable and trusted online environment" and address "the dissemination of illegal content online and the societal risks that the dissemination of disinformation [emphasis added] or other content may generate ". The DSA does not clearly define the notion of disinformation, but recital 106 makes a clear reference to the Code of Practice on Disinformation and establishes the complementary nature of the DSA and the Code (European Parliament and Council of the EU, 2022), thus incorporating the Code's broad definition of disinformation (Peukert, 2023).

In some circumstances, the proliferation of disinformation on social media platforms could constitute a "systemic risk" (Fahy, Appelman, and Helberger, 2022) under Article 34 of the DSA. This could be the case when (European Parliament and Council of the EU, 2022):

- certain forms of disinformation disseminated on the platform fall under the category of "illegal content" either at the EU or the Member State level;
- the disinformation has "any actual or foreseeable negative effects for the exercise of fundamental rights";
- the disinformation has "any actual or foreseeable negative effects on civic discourse and electoral processes, and public security";
- the disinformation has "any actual or foreseeable negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being".

The criteria outlined in Article 34 of the DSA highlight the significance of due diligence and risk assessment in addressing the proliferation of

disinformation on social media platforms. By categorizing certain forms of disinformation as "systemic risks", the DSA emphasizes the need for platforms to assess the potential negative impacts on fundamental rights, civic discourse, electoral processes, public security, and public health. This underscores how effective risk assessment and due diligence practices are not only essential for regulatory compliance but also reflect good business practices. Such approaches are in line with existing regulatory frameworks like the General Data Protection Regulation (GDPR) and cybersecurity regulations such as the NIS Directive, which impose a risk-based approach to data protection and cybersecurity, respectively. By integrating risk assessment into their operations, businesses can better identify, mitigate, and respond to threats posed by disinformation, thereby promoting trust, accountability, and resilience in the digital ecosystem.

Furthermore, due diligence serves as an inherently flexible standard designed to ensure technological neutrality and time resistance. This approach enables businesses to effectively address evolving digital challenges and emerging threats posed by disinformation. By embracing due diligence as a guiding principle, platforms can proactively identify and address risks, regardless of the specific technology or tactics employed by malicious actors. This dynamic framework allows for innovation while safeguarding fundamental rights and societal interests, fostering a resilient and trustworthy digital environment.

To prevent the aforementioned disinformation-related systemic risks, social media platforms have to "diligently identify, analyse and assess any systemic risks [emphasis added] in the Union stemming from the design or functioning of their service and its related systems". In order to mitigate associated risks, the platforms should, inter alia, "initiat[e] or adjus[t] cooperation with other providers of online platforms or of online search engines through the codes of conduct [emphasis added]". As specified in the DSA and the Code of Practice on Disinformation, signing up to all relevant Commitments under the Code may be considered as an appropriate risk-mitigating measure (European Parliament and Council of the EU, 2022; The Strengthened Code of Practice on Disinformation, 2022).

Although signing up to the relevant Commitments enshrined in the Code of Practice on Disinformation is voluntary, some provisions in the DSA indicate that non-participation in or non-compliance with the Code may incur legal liability. More specifically, recital 104 states that "[t]he refusal without proper explanations [...] of the Commission's invitation to

participate in the application of such a code of conduct" may be considered when determining whether an infringement of DSA obligations has occurred (European Parliament and Council of the EU, 2022).

If the Commission conclusively determines an infringement of the DSA obligations, it has the authority to impose fines up to 6% of the global turnover of the VLOP or VLOSE in question (Article 74 of the DSA). Additionally, the Commission can instruct the platform to implement measures to terminate or remedy the infringement within a specified deadline. This decision may initiate an enhanced supervision period to ensure the provider's compliance with the corrective measures (Article 75 of the DSA).

Hence, the DSA lays down strong incentives for platforms to adhere to the Code of Practice on Disinformation in order to mitigate liability risks, while the refusal to follow the Code could potentially expose platforms to infringement proceedings and fines (Maelen and Griffin, 2023).

Disinformation and media convergence – a rule of law issue. Lessons from Poland. In Poland, the legal framework governing media is primarily constituted by the Press Law dating back to 1984, alongside the Act on Radio and Television Broadcasting. Amendments made in 2011 aimed to align these laws with the European Audiovisual Media Services Directive. The plethora of national laws ensuring freedom of expression and access to information, together with the implementation of Poland's international commitments, ensure compliance with international and constitutional safeguards for freedom of expression in line with the European Convention on Human Rights and jurisprudence from the European Court of Human Rights. These legal instruments collectively establish the regulatory environment within which media operate, safeguarding the principles of free expression while also addressing contemporary challenges posed by evolving media landscapes.

Since the 2015 elections, Poland has encountered challenges to the rule of law, a phenomenon that has found its reflection also on social media. Despite the absence of dedicated legislation specifically targeting online platforms, there have been notable initiatives proposed to address concerns regarding freedom of expression in the digital sphere. One such proposal, advanced by the right-wing Minister of Justice, Zbigniew Ziobro in 2021, envisioned the introduction of a legislative act focusing on freedom of expression on platforms (Minister Sprawiedliwości, 2021). This draft proposal included a suggestion to establish a Council of Freedom of Expression for Social Media. It was designated to act as a local administra-

tive body, equipped with the authority to impose administrative fines over platforms that failed to comply with its decisions regarding the legality of content posted by individual users online. Such mandate would directly restrict the current authority of the independent, constitutional media authority that is the National Council of Radio and Television.

The latest version of the draft act also touched upon the issue of disinformation. It defined disinformation as false or misleading information that was produced, presented, and disseminated with the intention to obtain profit, undermine the public interest, or cause personal injury or property damage (Minister Sprawiedliwości, 2021). This definition was, by and large, in line with the Code of Practice on Disinformation.

Additionally, the draft act classified disinformation under the umbrella of "content of unlawful nature" (Minister Sprawiedliwości, 2021). Such classification somewhat deviates from the EU approach, which does not indiscriminately amount all types of disinformation to illegal content – in fact, the DSA sometimes clearly distinguishes the two categories by using the phrasing "illegal content or [emphasis added] disinformation" (European Parliament and Council of the EU, 2022, Recital 108). The distinction is significant because freedom of expression protects not only factually correct statements but also certain types of harsh and untruthful expressions – the so-called "awful but lawful" content (Appelman, Dreyer, Bidare, and Potthast, 2022). The balancing exercise must be carefully applied to address the issue of disinformation while ensuring the protection of freedom of expression and information.

Another initiative to counter disinformation suggested by the draft act was the establishment of a network of trusted flaggers. Trusted flaggers refer to state-certified entities with specialized knowledge to combat disinformation in public space, particularly in the fields of medicine, law, human rights, financial market, or public security. The objective of these certified entities was to submit complaints to the Council of Freedom of Expression regarding social media content containing disinformation. If the proceedings were to confirm that the content did constitute disinformation, the Council of Freedom of Expression would issue a respective decision ordering platforms to take it down. At the same time, considering the difficulties in determining what constitutes disinformation, the speed of disinformation dissemination on platforms, and time-consuming proceedings at the Council of Freedom of Expression, the question of the

effectiveness of such mechanism as a tool to counter disinformation remains open.

Although this draft is still pending with limited chances of approval, it underscores the ongoing struggle Poland faces in reconciling freedom of expression online with regulatory oversight and societal values.

Disinformation has emerged as a significant challenge in Poland, particularly during the period spanning 2015 to 2023, characterized by the monopolization of the national public media by the ruling right-wing party (Wójcik, 2023; Media Freedom Rapid Response, 2023). This dominance facilitated the dissemination of false information not only online but also through terrestrial networks. The negative impact of disinformation has proven to hold not only for online discourse but also for traditional media channels, posing substantial challenges to the rule of law and democratic processes. The manipulation of information ecosystems underscores the broader implications of disinformation beyond its digital manifestations, necessitating comprehensive strategies to safeguard public discourse and democratic principles in Poland.

As Poland strides toward democratic stability and restoring the rule of law, it offers the unique example of how vital media credibility and journalistic due diligence are for maintaining the rule of law. These recent lessons have shown the necessity for both traditional and digital media platforms to uphold consistent standards of integrity and accuracy.

Conclusions. The battle against disinformation presents a persistent challenge for European democracies, eroding trust in institutions and interfering with democratic processes. The rapid evolution of information and communication technologies, alongside the increasing influence of social media platforms as news sources, exacerbates this challenge. Russian disinformation campaigns, characterized by systematic dissemination and extensive use of social media, pose a significant threat to the European Union, particularly during pivotal events such as elections and demonstrations. Despite efforts to combat disinformation, including the establishment of the East StratCom Task Force and the EUvsDisinfo program, the problem persists, with Ukraine being a primary target of Russian disinformation. Strengthening the European media ecosystem is imperative, as evidenced by recent proposals such as the European Media Act, aiming to enhance regulatory frameworks and collaboration among stakeholders to counter disinformation effectively.

In Poland, the regulatory landscape governing media reflects a commitment to constitutional safeguards for free expression, aligning with European human rights standards. Despite facing challenges to the rule of law since the 2015 elections, including proposals for legislative acts on freedom of expression on platforms, Poland lacks dedicated laws addressing online platforms. Disinformation remains a critical issue, with the monopolization of national public media facilitating the spread of false information. Russian disinformation, regardless of the channel through which it is shared, presents a persistent challenge, highlighting the need for comprehensive strategies to safeguard democratic principles. Strengthening the European media ecosystem, possibly through initiatives like the European Media Freedom Act, is crucial to combatting disinformation effectively and preserving democratic values.

Addressing disinformation is not solely a matter of legal frameworks but requires a comprehensive, whole-of-society approach aimed at building resilience and enhancing capacity. While legal measures play a crucial role in regulating online platforms and combating disinformation, they must be complemented by efforts across various sectors, including education, media literacy, civil society engagement, and technological innovation. Building resilience involves empowering individuals to critically evaluate information, promoting transparency and accountability among online platforms, fostering collaboration among stakeholders, and leveraging technological advancements to detect and counter disinformation effectively. By adopting a holistic approach that engages all segments of society, countries can strengthen their resilience against the harmful effects of disinformation and uphold the principles of democracy and free expression in the digital age.

References:

1. Appelman, Naomi, Stephan Dreyer, Pranav Manjesh Bidare, Keno C. Potthast. 2022. "Truth, intention and harm: Conceptual challenges for disinformation-targeted governance". Internet Policy Review. https://policyreview.info/articles/news/truth-intention-and-harm-conceptual-challenges-disinformation-targeted-governance/1668

2. Commission on Security and Cooperation in Europe. 2017. "The Scourge of Russian Disinformation". https://www.csce.gov/hearings/scourge-russian-disinformation/

3. EU Code of Practice on Disinformation. 2018. https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation

4. European Commission and High Representative. 2016. Joint Framework on countering hybrid threats - a European Union response. April 6. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52016JC0018

5. European Commission and High Representative. 2018. Action Plan on disinformation. December 5. https://commission.europa.eu/document/download/b654235c-f5f1-452d-8a8c-367e603af841_en?filename=eu-communication-disinformation-euco-05122018_en.pdf

6. European Commission. 2018. Tackling online disinformation: a European Approach. April 26. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52018DC0236

7. European Commission. 2019. "A Europe that protects: good progress on tackling hybrid threats". Press corner. https://ec.europa.eu/commission/presscorner/detail/en/IP_19_2788

8. European Commission. 2020a. First baseline reports – Fighting COVID-19 disinformation Monitoring Programme. September, 10. https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme

9. European Commission. 2020b. Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement. September, 10. https://digital-strategy.ec.europa.eu/en/library/assessment-code-practice-disinformation-achievements-and-areas-further-improvement

10. European Commission. 2020c. On the European democracy action plan. December 3. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A52020DC0790

11. European Commission. 2021. Guidance on Strengthening the Code of Practice on Disinformation. May 26. https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation

12. European Commission. 2022. "The 2022 Code of Practice on Disinformation". Policies. https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation

13. European Commission. 2023. "Digital Services Act: Commission designates first set of Very Large Online Platforms and Search Engines".

Press corner. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_2413

14. European Council. 2015. European Council meeting – Conclusions. March 19-20. https://www.consilium.europa.eu/media/21888/european-council-conclusions-19-20-march-2015-en.pdf

15. European Digital Media Observatory. 2020. "Implementation of the Code of practice on disinformation: lessons from the assessments and proposals for the future". https://edmo.eu/wp-content/uploads/2021/02/EDMO_CoP_workshop281020_report-003.pdf

16. European External Action Service. 2021. "Questions and Answers about the East StratCom Task Force". https://www.eeas.europa.eu/eeas/questions-and-answers-about-east-stratcom-task-force_en

17. European Parliament and Council of the EU. 2022. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). October 19. https://eur-lex.europa.eu/eli/reg/2022/2065/oj

18. EUvsDisinfo. n.d. a. "About". Accessed January 12, 2024. https://euvsdisinfo.eu/about/

19. EUvsDisinfo. n.d. b. "Ukraine". Accessed January 10, 2024. https://euvsdisinfo.eu/ukraine/

20. Fahy, Ronan, Naomi Appelman, and Natali Helberger. 2022. "The EU's regulatory push against disinformation: What happens if platforms refuse to cooperate?" VerfBlog. https://verfassungsblog.de/voluntary-disinfo/

21. High level Group on fake news and online disinformation. 2018. "A multi-dimensional approach to disinformation". Publications Office of the EU. https://op.europa.eu/en/publication-detail/-/publication/6ef4df8b-4cea-11e8-be1d-01aa75ed71a1/language-en

22. Konarski, Xawery. 2022. "Dezinformacja online – jak ją rozumieć i jakie są środki prawne jej zwalczania w Polsce i UE". https://www.traple.pl/dezinformacja-online-jak-ja-rozumiec-i-jakie-sa-srodki-prawne-jej-zwalczania-w-polsce-i-ue/

23. Legucka, Agnieszka. 2019. "Countering Russian Disinformation in the European Union". Polish Institute of International Affairs. https://pism.pl/publications/Countering_Russian_Disinformation_in_the_European_Union

24. Maelen, Carl Vander, and Rachel Griffin. 2023. "Twitter's retreat from the Code of Practice on Disinformation raises a crucial question: are DSA codes of conduct really voluntary?" DSA Observatory. https://dsa-observatory.eu/2023/06/12/twitters-retreat-from-the-code-of-practice-on-disinformation-raises-a-crucial-question-are-dsa-codes-of-conduct-really-voluntary/

25. Media Freedom Rapid Response. 2023. "Report: Media freedom at a crossroads – Journalism in Poland faces uncertain future ahead of election". International Press Institute. https://ipi.media/report-media-freedom-at-a-crossroads-journalism-in-poland-faces-uncertain-future-ahead-of-election/

26. Minister Sprawiedliwości. 2021. Projekt ustawy o ochronie wolności słowa w internetowych serwisach społecznościowych, draft no. UD293. September 29. https://legislacja.rcl.gov.pl/projekt/12351757/katalog/12819467#12819467

27. Peukert, Alexander. 2023. "The Regulation of Disinformation in the EU – Overview and Open Questions". Research Paper of the Faculty of Law of Goethe University Frankfurt/M. No. 2/2023. https://ssrn.com/abstract=4496691

28. The Strengthened Code of Practice on Disinformation. 2022. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation

29. Wójcik, Anna. 2023. "Restoring Poland's Media Freedom". VerfBlog. https://verfassungsblog.de/restoring-polands-media-freedom/

30. Zadroga, Mateusz, and Magdalena Wilczyńska. 2023. "Disinformation landscape in Poland". EUvsDisinfo. https://www.disinfo.eu/wp-content/uploads/2023/12/20231203_PL_DisinfoFS.pdf