ZESZYT PRAWNICZY UAM
NR 14/2024
https://doi.org/10.14746/zpuam.2024.14.5

ISSN (ONLINE) 2956-2767
ISSN (PRINT) 2720-2526

JAKUB KOWALEWSKI

University of Lodz
https://orcid.org/0009-0006-1872-1836
jakub.kowalewski@edu.uni.lodz.pl

Global Disinformation Campaigns and International Law: Analyzing the Cases of Lisa and Confederation to Navigate the Complexities of Balancing Human Rights and National Security

Abstract: In the digital age, global disinformation campaigns are becoming a fundamental challenge that accompanies almost every conflict in international relations. The widespread adoption and development of such operations, especially those utilizing generative artificial intelligence, is inevitable. The article defines disinformation and locates it in the grid of near concepts. The author presents the ongoing conflict between the conduct of international actors and human rights, considering disinformation from the perspective of its adverse effects seen in their direct and indirect dimensions – through the consequences of the need to protect the national security of the targeted actors. Possible classification of the conduct of disinformation campaigns within the framework of public international law is also described and evaluated.

Keywords: public international law, disinformation, human rights, national security

Introduction

In 2020, the global Internet user base expanded to encompass over 4.6 billion individuals—a relative increase of 56% compared to the data from 2015.[1] The implications of this upsurge in international relations were far-reaching and could not have been overlooked, especially considering that the most significant increase related to the emerging and developing countries. In the European context, the countries that witnessed the most significant increase in Internet users over the past five years were Ukraine, Romania, and Belarus,[2] two of which are involved in an ongoing armed conflict, and all are considered to be developing economies (according to the IMF).[3] Overall, access to the Internet has created an environment conducive to the spread of disinformation that has continued to grow with the release of ChatGPT in 2022 and the increased availability of competing open-source generative artificial intelligence models (e.g., LLaMA, Pythia, PaLM2). These technological developments have brought new dynamism to international relations, creating previously unknown sources of influence that can be leveraged quickly and with limited resources. As

[1] Our World in Data, *Number of People Using the Internet* <https://ourworldindata.org/grapher/number-of-Internet-users> [accessed: 5.01.2024].

[2] Ibidem.

[3] *World Economic Outlook Database, Groups and Aggregates* <https://www.imf.org/en/Publications/WEO/weo-database/2023/April/groups-and-aggregates> [accessed: 29.02.2024].

a result, the issues of fake news and disinformation have become daily topics of discussion—there is an urgent need for education on trustworthiness and data verification, but also for decisive responses to protect national security.

This study aims to explore the negative impact of disinformation campaigns on human rights, focusing on differentiating between the direct impact caused by malicious actors and the indirect impact resulting from a state's efforts to safeguard its national security. To achieve this objective, we will delve into a detailed analysis of the definition of disinformation, providing a framework to understand the challenges in classifying such campaigns within the context of public international law. Two cases, a 15-year-old influenced by foreign propaganda, and a political party facing social media restrictions, are examined in this analysis.

1. Notions

According to an Independent High Level Group on Fake News and Online Disinformation, disinformation is "all forms of false, inaccurate, or misleading information designed, presented and promoted to intentionally cause public harm or for profit."[4] This definition articulates the goal of an entity that disseminates such information ("the cause of public harm or for profit") and leaves ground for communication that is not only false, but inaccurate or misleading. Several publications emphasize that disinformation goes beyond the publication of obviously false information and, often seeks to influence the recipient by suggesting what to believe.[5, 6] However, the source of the disinformation and how it is perceived is irrelevant, creating a substantial dissimilarity with the narrower definition of fake news—specific information that is false or distorted[7] and is likely to be perceived as news.[8] From this perspective, contemporary disinformation is predominantly used by entities that benefit from establishing credibility through means other than being recognized as a media outlet. Therefore, disinformation may derive from sources considered credible by its targets due to legal circumstances (state organs, media outlets) or social influence (e.g., politicians, trade unions, social media influencers). All in all, in international law, the terms

[4] European Commission, *A Multi-dimensional Approach to Disinformation: Report of the Independent High Level Group on Fake News and Online Disinformation*, 2018, p. 3.

[5] B. Baade, *Fake News and International Law*, "European Journal of International Law" 2018, vol. 29, no. 4, p. 1359.

[6] C. Espaliú-Berdud, *Use of Disinformation as a Weapon in Contemporary International Relations: Accountability for Russian Actions against States and International Organizations*, "El Profesional de la información" 2023, vol. 32, no. 4, pp. 5–7.

[7] B. Baade, op. cit., p. 1358.

[8] E. De Brabandere, *Propaganda*, [in:] A. Peters, R. Wolfrum (eds.), *The Max Planck Encyclopedia of Public International Law*, Oxford 2019 <https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e978> [accessed: 12.01.2024].

'disinformation' and 'fake news' can be comprehensively understood as distinct forms of propaganda—"a method of communication, by state organs or individuals, aimed at influencing and manipulating the behavior of people in a certain predefined way."[9]

The term disinformation campaign was notably used by the European Council to describe Russia's activities following the annexation of Crimea in 2014: this helps to clarify when disinformation becomes a campaign.[10] As Bryjka describes it, Russian propaganda efforts were engaged in constructing a narrative that served to rationalize territorial aggression—it portrayed Ukraine as an "'artificial state' devoid of any historical basis for its functioning and a by-product of poor decisions of the Soviet leadership."[11] The disinformation campaign that accompanied the aggression was so wide-ranging that it was aimed not only at the parties directly or indirectly involved in it but also at neutral countries (e.g., Japan,[12] Mali,[13] Mexico[14]). From these events, we can derive a criterion for identifying a disinformation campaign—it is an action with a certain level of organization and continuity that involves the dissemination of disinformation by a state or its agents and concerns conflict in the sphere of international relations.

2. Attribution to a State and Classification

To establish the relevance of disinformation in the context of international law, it is necessary to formulate a link between the dissemination of disinformation and a state. The general rule is abstracted from the *Draft articles on Responsibility of States for Internationally Wrongful Acts*—seen as to "be in whole or in large part an accurate codification of the customary international law of state responsibility"[15]—and is formulated as follows: "the only conduct attributable to the state in the international sphere is that of its public, executive, legislative, or judicial bodies, at any level of the administration, or that of others acting under the direction or control or at the instigation of those bodies—that is, as agents of the state."[16] When

[9] Ibidem.

[10] Council Conclusions of 19 and 20 March 2015, EUCO 11/15.

[11] F. Bryjka, *Russian Disinformation Regarding the Attack on Ukraine* <https://www.pism.pl/publications/russian-disinformation-regarding-the-attack-on-ukraine> [accessed: 7.01.2024].

[12] EUvsDisinfo, *The US Wants to Create a Military Bloc in Central Asia against Russia and China* <https://euvsdisinfo.eu/report/the-us-wants-to-create-a-military-bloc-in-central-asia-against-russia-and-china> [accessed: 14.01.2024].

[13] EUvsDisinfo, *France Is Supporting Terrorism in Mali* <https://euvsdisinfo.eu/report/france-is-supporting-terrorism-in-mali> [accessed: 14.01.2024].

[14] EUvsDisinfo, *Russia Is Winning against the Ukrainian Nazis and the West Is Doomed* <https://euvsdisinfo.eu/report/russia-is-winning-against-the-ukrainian-nazis-and-the-west-is-doomed> [accessed: 14.01.2024].

[15] J. Crawford, *State Responsibility: The General Part*, Cambridge 2013, p. 43.

[16] C. Espaliú-Berdud, op. cit., p. 7.

applied to known examples of disinformation in international relations, this concept strictly excludes all types of false information disseminated by entities that are not controlled or instigated by a state organ. As a result, sources that derive their credibility from legal status are most likely to be relevant under international law (e.g., government agencies, government-funded media), while sources that rely on social influence (e.g., social media influencers, politicians) would have to meet additional requirements that are often difficult or impossible to prove.

Once a disinformation campaign has been attributed to a State under the conditions described, it is necessary to determine whether disinformation interferes with international law and, if so, how. This is particularly difficult because, as Lahmann points out, there is no consensus on the issue. Disinformation campaigns can, therefore, violate the obligation to respect the sovereignty of other states and the prohibition of intervention, among other things.[17] An overview of both classifications allows further assessment of how disinformation might be viewed under international law.

2.1. Violation of Sovereignty

In terms of sovereignty, a fundamental principle of international law, the broadest interpretation of disinformation campaign can be derived from the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. The publication severely limits the scope for classifying a disinformation campaign as a violation of sovereignty—it emphasizes that two criteria should be considered: "the degree of infringement upon the target State's territorial integrity" and "whether there has been an interference with or usurpation of inherently governmental functions."[18] With respect to the first criterion, the *Manual* adheres to the interpretation that the territory of a state can be violated if physical damage or loss of functionality can be accounted for, including the violation of cyber infrastructure (both public and private) located within the territory of a state.[19] While it seems unreasonable to attribute physical damage to a disinformation campaign, it is feasible to attribute loss of functionality. As defined by Schmitt, this includes "rendering cyber infrastructure incapable of performing its functions in the manner intended."[20] A disinformation campaign with this kind of reach would most likely need to manipulate a large group of targets to take a given action over the Internet (e.g., visiting a particular website at a specific time, resulting in an effect like a DDoS operation, submitting comments

[17] H. Lahmann, *Infecting the Mind: Establishing Responsibility for Transboundary Disinformation*, "European Journal of International Law" 2022, vol. 33, no. 2, pp. 413–415.

[18] *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, M.N. Schmitt (ed.), Cambridge 2018, p. 20.

[19] M.N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, "Chicago Journal of International Law" 2018, vol. 19, no. 1, p. 43.

[20] Ibidem, p. 45.

or responses). The second criterion—interference or usurpation of inherently governmental functions—is an area in which a disinformation campaign cannot be considered. The provision of information, a function affected by disinformation, cannot be regarded as an inherently governmental function, regardless of the subject matter. Thus, disinformation campaigns can only be considered a violation of state sovereignty in a very narrow set of circumstances—those that result in the inability of an element of the state's infrastructure to perform its intended function.

2.2. Intervention

For disinformation to qualify as a state intervention, it must exert coercive pressure on a state, compelling it to act "involuntarily or refrain from acting in a certain way."[21] However, not all forms of pressure, such as economic pressure, are considered coercive under customary law.[22] This definition has a much broader scope than violating sovereignty as a basis for classifying a disinformation campaign.

Disinformation forcing a state to act in a particular way inherently was the 2020 Coronavirus campaign, which—as described by EUvsDisinfo—gave an impression of being "all over the place."[23] It sowed distrust in health care institutions and supported anti-vaccine movements across the EU. In 2021, Bulgaria's vaccination rate was the lowest in the bloc, and as Euronews frames it, the reason was "huge lack of confidence in public institutions." There is therefore a strong correlation between the disinformation campaigns targeted against Bulgarian society and the inability of the state to continue to promote vaccination (thus forcing the state to act in involuntary manner). If it is possible to attribute responsibility to a specific country according to the previously described requirements, then it would also be possible to qualify these activities as interventions.

3. Impact on Human Rights

Countering disinformation can have unintended consequences and often exacerbate the problem—this negative impact can be detrimental to human rights and democratic processes, as highlighted in a study conducted for the European Parliament.[24] This text presents an overview of the impact of disinformation on human rights from two perspectives: the conflict between human rights and actions of a state that is the

[21] B. Baade, op. cit., p. 1363.

[22] Ibidem.

[23] EUvsDisinfo, *The Kremlin and Disinformation about Coronavirus* <https://euvsdisinfo.eu/the-kremlin-and-disinformation-about-coronavirus> [accessed: 10.01.2024].

[24] C. Colomina, H. Sánchez Margalef, R. Youngs, *The Impact of Disinformation on Democratic Processes and Human Rights in the World*, Brussels 2022, pp. 9–12.

source of a disinformation campaign (direct impact) or a state that is targeted by it (indirect or response impact). Interpreting it in this manner allows for more careful consideration of the regulation of national security and how it, as an indirect effect of disinformation campaigns, raises new questions given the likely impossibility of holding the country initiating disinformation accountable.

The impact of disinformation on human rights is the most significant in relation to freedom of expression and the right to hold opinions without interference defined under Article 19 of legally binding International Covenant on Civil and Political Rights (ICCPR). In essence, the goal of disinformation is to exert psychological pressure and provide information that could influence the decision-making process of an entity—sowing division, confusion, and doubt, as framed by O'Shaughnessy.[25] These are in deep conflict with the provisions of the ICCPR and the essence of human rights. The 2016 Lisa case serves as a pertinent example of how certain human rights can be compromised, sparking a conflict between individuals and the state. The case—orchestrated by the Russian media, namely Sputnik and RT, and further propagated by state officials, including Russian Foreign Minister S. Lavrov—revolved around a campaign exploiting themes of xenophobia and the "rotten West." This disinformation, spread by Russian state-funded media outlets, accused German authorities of suppressing the case and hastily claimed that a Russo-German girl, identified as Lisa, had been sexually assaulted by men of immigrant origin.[26] The campaign manipulated public opinion by presenting distorted news and led to protests among the Russian minority in Germany.

It is important to note that the European legal framework provides a comprehensive approach to the right to freedom of expression and opinion without interference. This right is enshrined in both Article 11 of the Charter of Fundamental Rights of the European Union (CFR) and Article 10 of the European Convention on Human Rights (ECHR). The role of the latter in creating a positive obligation for states to protect against disinformation and to take countermeasures cannot be overstated, especially in light of recent developments in the case law of the European Court of Human Rights (*Association Burestop* judgment).[27]

3.1. Direct Impact

The direct impact of disinformation is understood as the effect resulting from the actions of a state conducting the disinformation campaign. With reference to

[25] N.J. O'Shaughnessy, *From Disinformation to Fake News: Forwards into the Past*, [in:] P. Baines, N.J. O'Shaughnessy, N. Snow (eds.), *The SAGE Handbook of Propaganda*, London 2020, pp. 58–60.

[26] B. Baade, op. cit., pp. 1359–1361.

[27] K. Pentney, *The Right of Access to 'Reliable' Information Under Article 10 ECHR: From Meagre Beginnings to New Frontiers*, "European Convention on Human Rights Law Review" 2024, vol. 5, no. 2, pp. 242–248.

the Lisa case cited above, the conflict that has been magnified by the direct impact of disinformation is how the rights of certain groups of individuals to freedom of thought and expression without interference have been violated. More broadly, it should be emphasized how Lisa's family's statements were used in a way that could be seen as an infringement of those individuals' right to privacy (Article 17 ICCPR). As Baade points out, Sputnik and RT were able to accuse state authorities of covering up the case because German police refused to comment on the case, citing privacy concerns.[28] This framing of the issue makes it possible to broaden the reflection by considering, inter alia, the Treaty on the Functioning of the European Union (TFEU), its Article 16 (right to privacy), and the corresponding Article 8 CFR. In the European Union's framework for the protection of fundamental rights, the right to privacy is clearly recognized as possessing a distinct and significant role.[29]

In the context of the right to privacy, the report *The impact of disinformation on democratic processes and human rights in the world* highlights that the right can be violated: "by damaging the individual reputation and privacy of the person it concerns in certain circumstances, and by failing to respect the privacy of individuals in its target audience."[30] Applying this to Lisa's case, it cannot be denied that the false narrative spread by the Russian media about the alleged assault severely damaged the reputation and privacy of the girl and her family. They were thrust into the center of a highly politicized incident, and their personal information and experiences were exploited for propaganda purposes. Article 16 TFEU provides the EU with the potential legal framework to address such violations through the implementation of proportionate measures.[31] The use of this framework is a positive obligation—to ensure that the rights of every individual, regardless of nationality, who falls within the scope of EU law are respected.[32] The EU should achieve this through legislation, the empowerment of independent authorities and the jurisprudence of the European Court of Justice.[33]

From Lisa's case, another example of the direct impact of disinformation on human rights can be abstracted—the violation of the right to freedom of expression (Article 19 ICCPR). Based on the data collected in the case by DFRLab, Russian media have "singled out individuals, such as Zeit columnist Alice Bota, who had criticized the Russian media's approach at the time, and outlets including Bild, which it accused of 'instrumentalizing the case of the abused girl for rabble-rousing against Russia.'" More than that, RT's article postulated that it "would surely be desirable if

[28] Ibidem.

[29] P.P. Craig, G. de Búrca, *EU Law: Text, Cases, and Materials*, New York 2020, p. 1045.

[30] C. Colomina, H. Sánchez Margalef, R. Youngs, op. cit., p. 11.

[31] H. Hijmans, *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*, Brussels 2016, pp. 24–25.

[32] M.G. Porcedda, *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*, Oxford and New York 2023, p. 111.

[33] H. Hijmans, *The European Union as Guardian of Internet Privacy*, op. cit., pp. 125–131.

the German mainstream media finally gave up their campaign on the case."[34] This can damage the professional reputations of individual reporters and encourage a practice of self-censorship, whereby a journalist refrains from reporting on similar issues to avoid further damage. This not only violates the individual's right to freedom of expression, but also affects the overall quality and diversity of news coverage. It is a significant concern because freedom of expression is considered a fundamental element of a functioning democracy.[35]

It should be assumed that direct influence is possible if a country is insufficiently prepared to counter disinformation. In Lisa's case, one can see the violation of numerous human rights in the face of the German population's unpreparedness to assess the information provided reliably and the unclear actions of German state bodies - malicious actors efficiently utilized these.

3.2. Indirect Impact (Response Impact)

The indirect impact of disinformation assesses the response of a country that is the target of a disinformation campaign. State security in sight of a disinformation campaign might necessitate a reassessment of specific human rights. It is worth noting that this may be done not only through statutes but also through soft law targeting private entities.[36] The second is the case of a non-binding set of guidelines (first published in 2018 and then reassessed in 2022) constituting the EU Code of Practice on Disinformation, which postulates to: "demonetize the dissemination of disinformation, ensure the transparency of political advertising, empower users, enhance cooperation with fact-checkers, and provide researchers with better access to data."[37] The document underlines the EU's strategic approach to mitigating disinformation—a strategy that does not prioritize complete eradication, but rather a cost-benefit shift. The EU aims to make quality information more accessible and affordable, while increasing the difficulty and effort of spreading disinformation.[38]

The case of Confederation, a Polish far-right political party, could be cited to illustrate the problem of the indirect impact of disinformation campaigns. Facebook removed the party's social media accounts in 2020 because the party disseminated COVID-19 disinformation, which was, at the time, an obvious avenue for multiple

[34] B. Nimmo, N. Aleksejeva, *Lisa 2.0* <https://medium.com/@DFRLab/lisa-2-0-133d44e8acc7> [accessed: 8.01.2024].

[35] C. Espaliú-Berdud, op. cit., pp. 10–11.

[36] J. van Hoboken, R.Ó. Fathaigh, *Regulating Disinformation in Europe: Implications for Speech and Privacy*, "UC Irvine Journal of International, Transnational, and Comparative Law" 2021, vol. 6, pp. 10–12.

[37] J. Kulesza, *Human Rights and Social Media: Challenges and Opportunities for Human Rights Education*, [in:] A. Mihr, C. Pierobon (eds.), *Polarization, Shifting Borders and Liquid Governance*, Cham 2024, p. 151.

[38] R. Arcos, I. Chiru, C. Ivan, *Routledge Handbook of Disinformation and National Security*, Abingdon, Oxon and New York, NY 2023, pp. 322–324.

malicious actors to pursue. Under the Commitment 14th of the 2022 EU Code of Practice on Disinformation, the service providers are required to "put in place or further bolster policies to address both misinformation and disinformation across their services." The application of this provision requires an assessment of how it affects the principle of political pluralism (Article 22 ICCPR), the right to hold opinions without interference (Article 19 ICCPR) and, in particular, as it concerns the exercise of the competence of EU institutions, the aforementioned right to privacy (under Article 17 ICCPR, Article 16 TFEU and Article 8 CFR). After a delay of a year and a half, Meta, owner of Facebook, decided to reactivate the profile of a political party, stating that "as a result of the WHO's announcement that the COVID-19 virus no longer poses a global health threat, and due to the upcoming parliamentary elections in Poland, we have determined that the public interest now outweighs the risk of direct harm posed by the profile."[39] The press release states that Meta has conducted a quasi-proportionality test after assessing the impact of restricting the party's political campaigning concerning COVID-19 and the close temporal proximity of political elections. Described behavior would have been expected of the company under both the 2018 Code and the later-signed 2022 Code; it is thus the desired effect of the EU encouraging measures to combat disinformation campaigns.

This practice, whereby the Union's institution encourages private entities to curtail expression, gives rise to concerns regarding its compatibility with the limitation clause set out in Article 19(3) of the ICCPR. The removal of a social media profile effectively represents a limitation on the right to freedom of expression without the clear foundation of a binding legal instrument; instead, the removal is justified through a reliance on a soft law mechanism. Moreover, it is indispensable to acknowledge that the scope of Article 19 of the ICCPR extends beyond the protection of accurate information; it also encompasses the right to express unpopular or even harmful views, which further intensifies the concerns regarding the case.[40] Considering that Confederation's electorate, more than any other Polish political party, consists of young voters,[41] such a corporate action negatively impacted political pluralism in Poland. On the other hand, by failing to make the decision, Meta would allow disinformation to flourish on its platform, compromising the right to freedom to hold opinions without interference. It was therefore a situation of conflict in which a political actor could simultaneously be seen as a political party itself, thus exercising its important role in the principle of political pluralism, while

[39] J. Czermiński, *Meta podjęła decyzję ws. profilu Konfederacji na Facebooku* [Meta has decided on the Konfederacja's Facebook profile] <https://www.rp.pl/polityka/art38582401-meta-podjela-decyzje-ws-profilu-konfederacji-na-facebooku> [accessed: 8.01.2024].

[40] M.L. Stasi, P.L. Parcu, *Disinformation and Misinformation: The EU Response*, [in:] P.L. Parcu, E. Brogi (eds.), *Research Handbook on EU Media Law and Policy*, Cheltenham 2021, p. 412.

[41] E. Karbowicz, *Kim są wyborcy partii politycznych w Polsce? Raport CBOS* [Who are the voters of political parties in Poland? CBOS Report] <https://www.gazetaprawna.pl/wiadomosci/kraj/artykuly/9244194,kim-sa-wyborcy-partii-politycznych-w-polsce-raport-cbos.html> [accessed: 8.01.2024].

at the same time being responsible for disseminating information that was harmful in the context of public health.

Within the framework of privacy rights, a key tension emerges in relation to the EU Code on Disinformation's emphasis on empowering fact-checkers. Giving third parties access to user data raises privacy concerns by expanding the data processing ecosystem, particularly by potentially incentivizing signatories to collect more user data than before. In general, this concern applies to any policy that makes use of user monitoring for the purpose of protection.[42] As highlighted in the Institute for Strategic Dialogue report, protecting privacy requires the development of a technological framework that facilitates anonymous data sharing while accommodating the large volumes of data involved.[43]

The case at hand highlights a significant concern regarding the authority of corporations and private entities when assessing the appropriateness of actions that could potentially violate human rights. This intricate matter demands a careful examination of private entities' role in shaping public discourse and the extent of their accountability for actions that may have a broader impact on society. It would be reasonable to entrust specific responsibilities to private entities while enabling state organizations to monitor their actions and intervene if necessary. Such oversight is nonexistent under the 2022 EU Code of Practice on Disinformation and should be considered in the following regulations.

Summary

Disinformation campaigns are reshaping the landscape of international law and politics, as they are both cost- and time-effective—they enable malicious actors to manipulate public sentiment and potentially tip the scales of political outcomes. In the past years, disinformation has profoundly impacted social capital worldwide, directly, and indirectly affecting human rights and democratic processes. In several cases, there was a correlation between a malicious campaign and a political trend (e.g., anti-vaccination, nationalism), or the latter directly resulted from the former (as in the 2016 Lisa case). The response of states targeted by these campaigns has highlighted the need to re-evaluate certain human rights in the context of national security, most notably the actors responsible for guaranteeing them. As of today, it is virtually impossible to hold a state accountable for conducting a disinformation campaign, particularly because of the difficulty of even attempting to attribute such actions to a state—most malicious actors will refuse to be associated with a country,

[42] J. van Hoboken, R.Ó. Fathaigh, op. cit., pp. 25–27.

[43] C. Colliver, *Cracking the Code: An Evaluation of the EU Code of Practice on Disinformation—ISD*, <https://www.isdglobal.org/isd-publications/cracking-the-code-an-evaluation-of-the-eu-code-of-practice-on-disinformation/> [accessed: 16.06.2024].

even if they receive direct funding from it (as RT is "autonomous" but "funded from the budget of the Russian Federation"[44]). Furthermore, categorizing the initiation of a disinformation campaign as a breach of legal responsibilities results in a domain of ambiguity that heavily relies on its consequences. The increasing prevalence of disinformation campaigns in the era of digitalization is a crucial concern in the field of international relations, bearing significant consequences for democratic processes and human rights. Numerous inquiries remain unresolved at the intersection of technological advancement and political impact.

BIBLIOGRAPHY

Arcos, R., Chiru, I., Ivan, C. (2023). *Routledge Handbook of Disinformation and National Security*, Abingdon, Oxon and New York, NY.

Baade, B. (2018). *Fake News and International Law*. "European Journal of International Law" 29(4): 1357–1376.

Colomina, C., Sánchez Margalef H., Youngs R. (2022). *The Impact of Disinformation on Democratic Processes and Human Rights in the World*. Brussels.

Craig, P.P., de Búrca G. (2022). *EU Law: Text, Cases, and Materials*. New York.

Crawford, J. (2013). *State Responsibility: The General Part*. Cambridge.

De Brabandere, E. (2019). *Propaganda*, [in:] A. Peters and R. Wolfrum (eds.), *The Max Planck Encyclopedia of Public International Law*. Oxford.

Espaliú-Berdud, C. (2023). *Use of Disinformation as a Weapon in Contemporary International Relations: Accountability for Russian Actions against States and International Organizations*, "El Profesional de la información" 32(4).

Hijmans, H. (2016). *The European Union as Guardian of Internet Privacy: The Story of Art 16 TFEU*. Brussels.

van Hoboken, J., Fathaigh, R.Ó. (2021). *Regulating Disinformation in Europe: Implications for Speech and Privacy*. "UC Irvine Journal of International, Transnational, and Comparative Law" 6: 9–36.

Kulesza, J. (2024). *Human Rights and Social Media: Challenges and Opportunities for Human Rights Education*, [in:] A. Mihr, C. Pierobon (eds.), *Polarization, Shifting Borders and Liquid Governance*. Cham: 139–154.

Lahmann, H. (2022). *Infecting the Mind: Establishing Responsibility for Transboundary Disinformation*, "European Journal of International Law" 33(2): 411–440.

O'Shaughnessy, N.J. (2020). *From Disinformation to Fake News: Forwards into the Past*, [in:] P. Baines, N.J. O'Shaughnessy, N. Snow (eds.), *The SAGE Handbook of Propaganda*. London: 55–70.

Pentney, K. (2024). *The Right of Access to 'Reliable' Information Under Article 10 ECHR: From Meagre Beginnings to New Frontiers*. "European Convention on Human Rights Law Review" 5(2): 230–267.

Porcedda, M.G. (2023). *Cybersecurity, Privacy and Data Protection in EU Law: A Law, Policy and Technology Analysis*. Oxford and New York.

Schmitt, M.N. (2018). *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*. "Chicago Journal of International Law" 19(1): 30–67.

Schmitt, M.N. (2018). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*. Cambridge.

Stasi, M.L., Parcu, P.L. (2021). *Disinformation and Misinformation: The EU Response*, [in:] P.L. Parcu, E. Brogi (eds.), *Research Handbook on EU Media Law and Policy*. Cheltenham: 407–426.

[44] RT, *About RT* <https://www.rt.com/about-us/> [accessed: 12.01.2024].