REVIEW OF EUROPEAN AND COMPARATIVE LAW
VOLUME XLVI
YEAR 2021, ISSUE 3, pp. 7–26
DOI: https://doi.org/10.31743/recl.12389

INFORMATION POLLUTION IN A DIGITAL AND POLARIZED WORLD AS A CHALLENGE TO HUMAN RIGHTS PROTECTION – THE COUNCIL OF EUROPE'S APPROACH

*Alicja Jaskiernia**

ABSTRACT

Information pollution in a digitally connected and increasingly polarized world, the spread of disinformation campaigns aimed at shaping public opinion, trends of foreign electoral interference and manipulation, as well as abusive behaviour and the intensification of hate speech on the internet and social media are the phenomenon which concern international public opinion. These all represent a challenge for democracy, and in particular for the electoral processes affecting the right to freedom of expression, including the right to receive information, and the right to free elections. It is a growing international effort to deal with these problems. Among international organizations engaged to seek solutions is the Council of Europe (CoE). The author analyses CoE's instruments, legally binding (as European Convention on Human Rights), as well of the character of "soft law", especially resolution of the CoE's Parliamentary Assembly 2326 (2020) *Democracy hacked? How to respond?* She exposes the need for better cooperation of international organizations and states' authorities in this matter.

Keywords: information pollution, disinformation campaigns, hate speech, democracy, Council of Europe

* Prof. Dr. habil. Alicja Jaskiernia, Professor, Faculty of Journalism, Information and Book Studies, University of Warsaw; correspondence address: ul. Bednarska 2/4, 00-310 Warszawa, Poland; e-mail: a.jaskiernia@uw.edu.pl; https://orcid.org/0001-0001-8412-7217.

1. INTRODUCTION

How do we make sense of digitizing cultures?[1] Information pollution in a digitally connected and increasingly polarized world, the spread of disinformation campaigns aimed at shaping public opinion, trends of foreign electoral interference and manipulation, as well as abusive behaviour and the intensification of hate speech on the internet and social media are the phenomenon which concern international public opinion[2]. These all represent a challenge for democracy, and in particular for the electoral processes affecting the right to freedom of expression[3], including the right to receive information, and the right to free elections[4]. They need adequate legal procedures to cope with[5] the situation. The ubiquity of the Internet contrasts with the territorial nature of national legal orders[6]. However, there is a growing international effort to deal with that problem. There are important EU Internet regulatory challenges currently found in various key fields of law directly linked to the Internet such as information technology, consumer protection, personal data, e-commerce and copyright law[7].

The growth of Information and Communication Technology (ICT) and the prevalence of mobile devices make cyber security a highly topical and relevant issue. The transition from 4G to 5G mobile communication, while bringing convenience, also means cyber threats are growing

[1] Thomas Vernon Reed, *Digitized lives: culture, power, and social change in the internet era* (New York: Routledge, 2019), 24.

[2] James Ball, *The system: who owns the internet, and how it owns us* (London: Bloomsbury Publishing, 2020), 33.

[3] Susi Susi, ed., *Cyber Security: The Lifeline of Information and Communication Technology* (London, New York: Routledge, Taylor & Francis Group, 2019).

[4] Lilian Edwards, *Law, policy and the Internet* (Oxford: Hart, 2019), 34.

[5] Graham Smith, Ruth Boardman, Flynn Cathal, Gabe Maldoff, *Internet law and regulation* (London: Sweet & Maxwell, 2020), 51.

[6] Pedro de Miguel Asensio, *Conflict of laws and the internet* (Cheltenham, England, Northampton, Massachusetts: Edward Elgar Publishing, 2020), 32.

[7] Tatiana-Eleni Synodinou, Philippe Jougleux, Christiana Markou, Thalia Prastitou, eds., *EU Internet Law in the Digital Era Regulation and Enforcement* (Cham: Springer International Publishing, 2020).

exponentially[8]. As regards cyberattacks, international organizations raised concerns[9] in particular with regard to numerous cases of mass disinformation campaigns intended to undermine security, public order and peaceful democratic processes, and to the need to develop tools to protect democracy from "information weapons"[10]. The studies are held to analyze phenomenona of Internet' content, including memes[11]. The analysis of the problem of information pollution is of particular importance in the context of the protection of the freedom of information, guaranteed, *inter alia*, by art. 10 of the European Human Rights Convention. Thus, it is of great importance in the context of the international system of human rights protection in all aspects of the functioning of political systems which depend on the full guarantee of freedom of expression.

The occasion to analyze this problem led to the creation of resolution 2326 (2020) of the Council of Europe Parliamentary Assembly entitled *Democracy hacked? How to respond?* in which it was stressed that:

> The Parliamentary Assembly is concerned about the scale of information pollution in a digitally connected and increasingly polarized world, the spread of disinformation campaigns aimed at shaping public opinion (…)[12].

As the Internet and social media seep into ever more aspects of the political landscape, the Assembly points to the need to improve the Internet's content and architecture, build up the resilience of Europe's democratic systems and societies, counter disinformation, invest in quality journalism and preserve freedom of expression and media and political pluralism, es-

---

[8] Vandana Rohokale, *Cyber Security: The Lifeline of Information and Communication Technology* (Cham: Springer International Publishing, 2020), 44.

[9] PACE Resolution 2217 (2018) and Recommendation 2130 (2018) on legal challenges related to hybrid war and human rights obligations.

[10] Mohiuddin Ahmed, Abu S. S. M. Barkat Ullah, and Al-Sakib Khan Pathan, eds., *Security analytics for the internet of everything* (Boca Raton, Florida, London, New York: CRC Press, 2020).

[11] Anastasia Denisova, *Internet memes and society: social, cultural, and political contexts* (New York, London: Routledge, 2019), 43.

[12] *Assembly debate* on 31 January 2020 (9th Sitting) (see Doc. 15028, report of the Committee on Political Affairs and Democracy, rapporteur: Mr. Frithjof Schmidt; and Doc. 15056, opinion of the Committee on Legal Affairs and Human Rights, rapporteur: Mr. Emanuelis Zingeris). *Text adopted by the Assembly* on 31 January 2020 (9th Sitting).

pecially in the context of elections. It is worth analyzing that document in the broader perspective of challenges which bring about information pollution and activities of the Council of Europe to confront that problem.

The aim of this publication is to analyze the phenomenon of information pollution, and in particular the problem of threats which it brings about to the freedom of information perceived as a crucial human right and as an important premise for the functioning of democratic systems. The following hypothesis will be verified: contaminated information poses a threat to the realization of the freedom of speech and more effective involvement of national and international instruments are needed to combat this phenomenon. The following research methods will be used in the work: institutional and legal, legal-comparative and system analysis.

2. GENERAL CHARACTERISTICS OF THE PHENOMENON OF INFORMATION POLLUTION

Information pollution (also referred to as "info pollution") is the contamination of information supply with irrelevant, redundant, unsolicited, hampering and low-value information[13]. Information pollution generally applies to digital communication, such as e-mail, instant messaging (IM) and social media. The term acquired particular relevance when web expert Jakob Nielsen published an essay in which he raised questions surrounding the concept of "information pollution", exposing the negative side of the global trend of empowering internet users to access and produce "knowledge"[14]. The spread of useless and undesirable information can have a detrimental effect on human activities. It is considered one of the adverse effects of the information revolution. Nowadays researchers were expressing doubts about the negative effects of overloading of information seen as the digital equivalent of the environmental pollution generated by indus-

[13] Levent Orman, "Fighting Information Pollution with Decision Support Systems," *Journal of Management Information Systems* 1, no. 2 (2015): 65.

[14] Jakob Nielsen, "IM, Not IP (Information Pollution): A steady dose of realtime interruptions is toxic to anyone's health," November 2003, Association for Computing Machinery, https://dl.acm.org/doi/pdf/10.1145/966712.966731, accessed March 23, 2021.

trial processes. The new terms of information pollution like "disinfomedic" or "infodemic", have occurred as a term to describe the role of social media in the pandemic of COVID-19. The broader notion of these terms stress the possible negative influence to people who live in a "mediated reality constructed out of fake news, misinformation, rumours and lies"[15].

In recent years, data protection has become a major concern in many countries, as well as at supranational and international levels. In fact, the emergence of computing technologies that allow lower-cost processing of increasing amounts of information, associated with the advent and exponential use of the Internet and other communication networks and the widespread liberalization of the cross-border flow of information have enabled the large-scale collection and processing of personal data, not only for scientific or commercial uses, but also for political uses. A growing number of governmental and private organizations now possess and use data processing in order to determine, predict and influence individual behavior in all fields of human activity. This inevitably entails new risks, from the perspective of individual privacy, but also other fundamental rights, such as the right not to be discriminated against, fair competition between commercial enterprises and the proper functioning of democratic institutions. These phenomena have not been ignored from a legal point of view: at the national, supranational and international levels, an increasing number of regulatory instruments – including the European Union's General Data Protection Regulation applicable as of 25 May 2018 – have been adopted with the purpose of preventing personal data misuse. Nevertheless, distinct national approaches still prevail in this domain, notably those that separate the comprehensive and detailed protective rules adopted in Europe since the 1995 Directive on the processing of personal data from the more fragmented and liberal attitude of American courts and legislators in this respect[16].

The internet isn't the first technology to alter how we communicate, but it is making our language change faster and in more interesting ways

[15] Mark Deuze, "The Role of Media and Mass Communication Theory in the Global Pandemic," *Communication Today* 11, no. 2 (2020): 9.

[16] Vicente Dário Moura and Sofiade Vasconcelos Casimiro, eds., *Data Protection in the Internet* (Cham: Springer International Publishing, 2020).

than ever before. The programmers behind the apps and platforms we use decide how our conversations are structured, from the grammar of status updates to the protocols of comments and @replies. Linguistically inventive niche online communities spread slang faster than in the days when new dialects were constrained by offline space[17].

A compelling argument that the Internet of things threatens human rights and security and that suggests policy prescriptions to protect our future. The Internet has leapt from human-facing display screens into the material objects all around us. In this so-called Internet of Things – connecting everything from cars to cardiac monitors to home appliances – there is no longer a meaningful distinction between physical and virtual worlds. Everything is connected[18]. The Internet of Things (IoT) is the notion that nearly everything we use, from gym shorts to streetlights, will soon be connected to the Internet; the Internet of Everything (IoE) encompasses not just objects, but the social connections, data, and processes that the IoT makes possible. As more devices and systems become intertwined, the growing scale of the threat from hackers can easily get lost in the excitement of lower costs and smarter tech[19]. Thanks to rapid advances in sensors and wireless technology, Internet of Things (IoT)-related applications are attracting more and more attention. As more devices are connected, they become potential components for smart applications. Thus, there is a new global interest in these applications in various domains such as health, agriculture, energy, security and retail[20]. From new ways of negotiating privacy, to the consequences of increased automation, the Internet of Things poses new challenges and opens up new questions that often go beyond the technology itself, and rather focus on how the technology

[17] Gretchen McCulloch, *Because Internet: understanding the new rules of language* (New York: Riverhead Books, 2019), 38.

[18] Laura DeNardis, *The Internet in Everything: Freedom and Security in a World with No Off Switch* (New Haven, CT: Yale University Press, 2020), 52.

[19] Scott J. Shackelford, *The Internet of Things: What Everyone Needs to Know* (New York: Oxford University Press, 2020), 48.

[20] Valentina E. Balas, Vijender Kumar Solanki, and Raghvendra Kumar, eds., *Internet of Things and Big Data Applications Recent Advances and Challenges* (Cham: Springer International Publishing, 2020).

will become embedded in our future communities, families, practices, and environment, and how these will change in turn[21].

The publicly available datasets are outlined along with experimental settings. Internet and social media have become a widespread, large scale and easy to use platform for real-time information dissemination. It has become an open stage for discussion, ideology expression, knowledge dissemination, emotions and sentiment sharing. This platform is gaining tremendous attraction and a huge user base from all sections and age groups of society of the digital economy era, when technologies "mediate time"[22]. The matter of concern is that up to what extent the contents that are circulating among all these platforms every second changing the mindset, perceptions and lives of billions of people are verified, authenticated and up to standards[23].

Employees are facing information explosion in the presence of destructive information and communication technologies of industry 4.0. With the prevalent nature of information pollution, employees are finding it difficult to process large volume of information in order to access quality information. The perceived information pollution comprises five dimensions – accessible, intrinsic, contextual, representational, and distractive information pollution. With new quantum technology, hacker-proof exchange of information and ultrafast data processing will become possible. The basis for these is Albert Einstein's "quantum spook". We are not dealing here with witchcraft, but with hard-core science[24].

---

[21] Alessandro Soro, Margot Brereton, and Paul Roe, eds., *Social Internet of Things* (Cham: Springer International Publishing, 2019).

[22] Bohdan Jung and Tadeusz Kowalski, "Restructuring Time Use Under COVID-19 Pandemics," *International Journal of Inspiration & Resilience Economy* 5(1) (2021): 23; Priyanka Meel and Dinesh Kumar Vishwakarma, "A temporal ensembling based semi-supervised ConvNet for the detection of fake news articles," *Expert Systems with Applications* 177 (2021): 115002.

[23] Priyanka Meel and Dinesh Kumar Vishvakarma, "Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities," *Expert Systems with Applications* 153 (2020): 112986.

[24] Gösta Fürnkranz, *The Quantum Internet Ultrafast and Safe from Hackers* (Cham: Springer International Publishing, 2020), 19.

3. THE COUNCIL OF EUROPE'S ACTIVITY AGAINST INFORMATION POLLUTION

The Council of Europe several times analyzed the phenomenon of information pollution. Internet intermediaries, including social media, play a crucial role in providing services of public value and facilitating public discourse and democratic debate. Council of Europe standards set out the intermediaries' responsibilities with respect to ensuring human rights and fundamental freedoms on their platforms, which includes the right to free elections. In this regard, internet intermediaries should be subject to effective oversight and regular due diligence assessments of their compliance with their responsibilities[25].

In 2002, the Venice Commission adopted the Code of Good Practice in Electoral Matters[26] which ensures electoral equity and equality of opportunity. This applies, in particular, to radio and television air-time, public funds and other forms of backing and entails a neutral attitude by State authorities, in particular with regard to election campaigns, media coverage, especially by publicly owned media, and public funding of parties and campaigns. However, the Code also states that "legal provision should be made to ensure that there is a minimum access to privately owned audio-visual media, with regard to the election campaign and to advertising, for all participants in elections" and that "the principle of equality of opportunity can, in certain cases, lead to a limitation of political party spending, especially on advertising". Furthermore, important work is being done by the Venice Commission, which, on 24 June 2019, adopted a joint report, with the Directorate of information society and action against crime, on Digital technologies and elections, which proves relevant to my analysis. The Venice Commission also decided to prepare a list of principles for the use of digital technologies in a human rights compliant manner, in relation to elections.

In 2011, PACE adopted Resolution 1843 (2011) and Recommendation 1984 (2011) on "The protection of privacy and personal data on

[25] Venice Commission, "Joint Report on Digital Technologies and Elections", CDL-AD(2019)016; 24/06/2019, 5,8; CDL-LA(2018)002,9.

[26] Venice Commission, Opinion No. 190/2002.

the Internet and online media". The resolution emphasized that the protection of the right to data protection is a necessary element of human life and of the humane functioning of a democratic society, and that its violation affects a person's dignity, liberty and security.

In 2012, the Committee of Ministers of the Council of Europe adopted two relevant Recommendations on the protection of human rights with regard to search engines and social networking services. In the first text, the Committee of Ministers recognized the challenge caused by the fact that an individual's search history contains a footprint which may reveal the person's beliefs, interests, relations or intentions, and could reveal, *inter alia*, one's political opinions or religious or other beliefs. The Recommendation called for action to enforce data protection principles, in particular purpose limitation, data minimization and limited data storage, while data subjects must be made aware of the processing and provided with all relevant information[27].

Concerned with the interference of the right to private life by rapid technological developments, in 2013 the Committee of Ministers of the Council of Europe adopted a *Declaration on risks to fundamental rights stemming from digital tracking and other surveillance technologies*[28].

In 2017, the Council of Europe report on *Information disorder: Toward an interdisciplinary framework for research and policy making*, which suggests ways to determine the type of response suited to the threat. As the concept of "fake news" is too imprecise, the report makes a distinction between: misinformation – when false information is shared, but no harm is meant; disinformation – when false information is knowingly shared to cause harm; malinformation – when genuine information is shared to cause harm, by transferring it from private into the public sphere. The report points out that our societies need:

– in the short term, to address the most pressing issues, for instance around election security;
– in the long term, to increase society's resilience to disinformation;
– a structure capable of checking and constantly adapting responses[29].

[27] Recommendation CM/Rec (2012)3.

[28] https;/RM.coe.int/168068460d, accessed March 12, 2021.

[29] *Council of Europe Report on Information and Disorder* (Strasbourg: Council of Europe, 2017): 3.

Under the European Convention on Human Rights, as interpreted by the European Court of Human Rights, member States have an obligation to secure the rights and freedoms for everyone within their jurisdiction, both offline and online. Article 10 of the European Convention on Human Rights, which guarantees freedom of information, is fundamental to the protection of human rights in relation to freedom of expression in the member states of the Council of Europe. The crucial issue is to determine whether the obligations of the State in assuring equal publicity of political parties and candidates are to be applied to internet intermediaries and if so, in what manner. In this regard, the Committee of Ministers' Recommendation CM/Rec (2018)1 on media pluralism and transparency of media ownership and Recommendation CM/Rec (2018)2 on the roles and responsibilities of Internet intermediaries, point to the potentially disturbing impact that online platform's control over the flow, availability, findability and accessibility of information can have on media pluralism. The Committee of Ministers called on member States to act as the ultimate guarantor of media pluralism by ensuring pluralism in the entirety of the multimedia ecosystem.

The 15th Conference of Electoral Management Bodies on Security in Elections, organized by the Venice Commission on 19 and 20 April 2018, showed clearly that the right to free suffrage was facing digital challenges in two respects: voters' freedom to form an opinion and their freedom to express their will. It was also stressed that while criminal penalties should apply to cyberattacks, the effectiveness of judicial responses to date was relatively limited[30].

In the Declaration on the manipulative capabilities of algorithmic processes adopted on 13 February 2019, the Committee of Ministers of the Council of Europe called on its 47 member States to tackle the risk that individuals may not be able to form their opinions and take decisions independently of automated systems, and that they may even be subjected to manipulation due to the use of advanced digital technologies, in particular micro-targeting techniques. Machine learning tools have the growing capacity not only to predict choices but also to influence emotions and thoughts, sometimes subliminally. The Committee encouraged member

[30] Website of the 15th European Conference on Electoral Management Bodies.

States to assume their responsibility to address this growing threat in particular by taking appropriate and proportionate legislative measures against illegitimate interferences, and empowering users by promoting critical digital literacy skills. The Committee went as far as stressing the need to assess the regulatory frameworks related to political communication and electoral processes to safeguard the fairness of elections and to ensure that voters are protected against unfair practices and manipulation. It also stressed the significant power that technological advancement confers to those who may use algorithmic tools without adequate democratic oversight or control and underlined the responsibility of the private sector to act with fairness, transparency and accountability under the guidance of independent public institutions[31].

As regards cyberattacks, the Parliamentary Assembly of the Council of Europe has raised concerns in Resolution 2217 (2018) and Recommendation 2130 (2018) on legal challenges related to hybrid war and human rights obligations, in particular with regard to numerous cases of mass disinformation campaigns intended to undermine security, public order and peaceful democratic processes, and to the need to develop tools to protect democracy from "information weapons".

The work that has been done by the Council of Europe on personal data protection and electoral rights, especially the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108, Convention 108) and its relevance with regard to electoral rights, welcomes other *soft law* instruments addressing different aspects of privacy and personal data protection in the context of the information society, including in social networks. The Protocol amending the Convention (CETS No. 223) modernizes the convention and addresses emerging challenges resulting from the use of new information and communication technologies, and supports the call of the United Nations' Special Rapporteur on the right to privacy. The Convention 108 on the use of personal data in elections and their possible misuse in a political context continues this activity.

On social networks, the Committee of Ministers of the Council of Europe recommended that member States take actions to provide an en-

[31] CM Declaration on the manipulative capabilities of alghoritmic processes.

vironment for users of social networks that allows them to further exercise their rights and freedoms, to raise users' awareness of the possible challenges to their human rights and of the negative impact on other people's rights when using these services, as well as to enhance transparency about data processing, and forbids the illegitimate processing of personal data[32].

The Council of Europe has invited its member States that have not already done so to sign and/or ratify and fully implement the Council of Europe Convention on Cybercrime (ETS No. 185) and its Additional Protocol concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems (ETS No. 189).

The Parliamentary Assembly of the Council of Europe has appointed Mr. Frithjof Schmidt (Germany, Socialist) to be rapporteur for preparation of the rapport *Democracy hacked? How to respond?*[33] for the Committee on Political Affairs and Democracy, which was a base for the PACE's resolution 2326 (2020). The rapporteur has analyzed the following questions: does the introduction of digital public structures threaten our public debates and current model of representative democracies? How can we increase society's resilience to disinformation? Is there not a risk that the way social media operates, by accentuating what researchers call "cocooning", i.e. the tendency of connected groups of individuals to keep to themselves and only follow "news", whether true or false, that confirms their points of view, as well as the business logic of platform operators and the lack of transparency in information distribution will cut these groups of web users off from confronting views they do not share? In other words, if democracy involves acceptance of debate among people who hold different views, does this trend render this aspect of democracy obsolete?[34] He found that the relationship between democracy and a new technological environment is a complex one. On the one hand, the internet and social media have become a central platform of political interaction. In some democracies, the use of technology tools has facilitated democratic participation and political activism. On the other hand, internet and social

[32] Recommendation CM/Rec (2012)4.

[33] PACE, Reference to committee: Bureau decision, Reference 4353 of 22 January 2018. 2020 - First part-session, Doc. 15028.

[34] PACE, Explanatory memorandum by Mr. Frithjof Schmidt, Doc. 15028, § 1.2.

media can endanger the voters' free will or the principle of equal opportunities for all candidates as well as voters' rights to privacy. As a matter of fact, the increase of content production and the centralization of online distribution channels by a few companies (Twitter, Google and Facebook) have had several unintended consequences: the proliferation of private and public disinformation tactics, and most importantly, the arrival of non-regulated private actors in the democratic arena. These new players are literally "owners" and new "gatekeepers" of the global communication infrastructure. Virtual tools can be used as a threat for the integrity of the elections in several ways, such as suppressing voter turnout, tampering with election results, stealing voter information, conducting cyberespionage or doxing of candidates for the purposes of manipulation and shaping the opinions of voters. In relation to defense, cyberattacks are becoming increasingly significant in what is now called "hybrid warfare", a new type of warfare combining conventional and non-conventional methods. This also involves a redefinition of conventional military strategy concepts of attack and defense. In this context, there is a great risk of civil society being targeted directly and its rights being jeopardized. The importance of this issue is without doubt[35].

According to Freedom House, manipulation and disinformation tactics played an important role in elections in at least 18 countries in 2017, damaging citizens' ability to choose their leaders based on factual news and authentic debate and giving rise to what has been named "digital authoritarianism". At the same time, governments around the world are tightening control over citizens' data and using claims of "fake news" to suppress dissent, eroding trust in the internet as well as the foundations of democracy[36]. In January 2018, Swedish security chief Anders Thornberg, in the context of the general elections in Sweden, pointed to several ex-

[35] Ibidem, § 1.3–5.

[36] Freedom House, *Freedom on the Net 2018, the rise of digital authoritarianism*, https://www.google.pl/search?ei=hcFMYP3SJuH6qwH9qonQDg&q=Freedom+House%2C+Freedom+on+the+Net+2021%2C+the+rise+of+digital+authoritarianism&oq=Freedom+House%2C+Freedom+on+the+Net+2021%2C+the+rise+of+digital+authoritarianism&gs_lcp=Cgdnd3Mtd2l6EAw6BwgAEEcQsANQqyVYsDtgwUtoAXACeACAAYcCiAH8BJIBBTMuMS4xmAEAoAEBqgEHZ3dzLXdpesgBCLgBAsABAQ&sclient=gws-wiz&ved=0ahUKEwi9qaWfs63vAhVh_ SoKHX1VAuoQ4dUDCAw, accessed March 13, 2021.

amples of fake news articles that sought to create division and undermine trust, including one that claimed that Muslims had vandalized a church. The latter was spread, using bots, which were from outside Sweden. He pointed out the national security implications when a foreign actor uses such disinformation campaigns. In January 2019, Facebook took down two large-scale disinformation operations linked to Russian State actors operating across Eastern and Central Europe. In February 2019, the German authorities arrested a 20-year-old student who confessed to having illegally accessed information on more than 1 000 public figures, including high-ranking politicians. In November 2019, Facebook announced that it had removed 5.4 billion fake accounts throughout the year[37]. Built as an open and democratic space, the internet is a global village allowing information to spread easily at low cost. Therefore, it is difficult to identify trustworthy information or find those responsible for illegal actions online. Online propaganda, disinformation and hate-speech have increased in the digital sphere. In this context, guaranteeing the freedom of voting and fair elections, while preserving freedom of expression, represents a major challenge. If citizens are unable to distinguish between false and true data and are unaware of the conditions under which they exercise their rights and freedoms, the purity of their will might be compromised, as well as the democratic legitimacy of the elections themselves[38]. Experts claim that misinformation, sometimes backed by governments, has already influenced several major events in Europe. For example, some claim that disinformation may have influenced the Dutch vote on the EU-Ukraine Association Agreement, the result of the Brexit vote, the debates around the independence of Catalonia, and immigration issues in Italy. According to the Final Report of the UK House of Commons' Digital, Cultural, Media and Sport Committee of 14 February 2019, following an 18-month investigation into disinformation, "democracy is at risk from the malicious and relentless targeting of citizens with disinformation and personalized 'dark adverts' from unidentifiable sources, delivered through the major so-

[37] https:/editoion.ccon.com/2019/11/13/tech/facebo ok.-take-accounts/index.html, accessed March 13, 2021.

[38] CDL-LA(2018)001; 21/11/2018,9.

cial media platforms"[39]. Furthermore, according to a Venice Commission study, the use of artificial intelligence (AI) during election campaigns raises ethical and democratic questions as there is evidence and further possibility to use them to manipulate citizens and influence the electoral results[40].

4. RECOMMENDATIONS OF THE PARLIAMENTARY ASSEMBLY OF THE COUNCIL OF EUROPE ADDRESSING DISINFORMATION CHALLENGES

In resolution 2326 (2020) the Parliamentary Assembly of the Council of Europe addressing disinformation challenges in the context of democratic elections, recommended that governments of the Council of Europe member States need to: a) recognize the transnational nature of the problem and enhance co-operation with internet intermediaries and social media operators, whose commercial interests tend to collide with human rights and political rights, for instance the principle of electoral equity, in line with the Committee of Ministers Recommendation CM/Rec(2018)2 on the roles and responsibilities of Internet intermediaries; b) enable voters to receive trustworthy information and become more informed and engaged, with a view to preserving the exercise of their right to truly free and fair elections; c) break up the monopoly of technology companies controlling, to a great extent, citizen's access to information and data; d) consider updating national legislation in order to counter disinformation campaigns more effectively[41].

To tackle these challenges, the Assembly has called on Council of Europe member States to implement a number of strategies from a European and global perspective and to create a model that includes co-responsibility and multiple regulatory and conflict-resolution approaches, in particular by: a) promoting media education and digital literacy skills to strengthen the legal and democratic culture of citizens, in line with Reso-

[39] https:/publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm, accessed March 13, 2021.

[40] PACE, Explanatory memorandum…, § 2.12–18.

[41] PACE Res. 2326 (2020), § 5.

lution 2314 (2019) on media education in the new media environment, enhance public awareness of how data are generated and processed, enable voters to evaluate critically electoral communication and increase society's resilience to disinformation; b) encouraging and supporting collaborative fact-checking initiatives and other improvements of content moderation and curation systems which are intended to counter the dissemination of deceptive and misleading information, including through social media, in line with Resolution 2281 (2019) "Social media: social threads or threats to human rights?"; c) securing adequate funding to independent public service media, so that the media can allocate enough resources to innovate in content, form and technology to foster their role as major players in countering disinformation and propaganda and as cutting-edge stakeholders in protecting communication and media ecosystems in Europe, in line with Resolution 2255 (2019) on public service media in the context of disinformation and propaganda; d) strengthening transparency in political online advertising, information distribution, algorithms and business models of platform operators, in particular by: guaranteeing, where political parties and candidates have the right to purchase advertising space for election purposes, equal treatment in terms of conditions and rates charged; developing specific regulatory frameworks for internet content at election times and including provisions on transparency in relation to sponsored content on social media, so that the public is aware of the source that funds electoral advertising or any other information or opinion, in line with Resolution 2254 (2019) on media freedom as a condition for democratic elections, and prevent illegal foreign involvement; e) addressing the implications of the micro-targeting of political advertisements with a view to promoting a political landscape which is more accountable and less prone to manipulation; f) supporting researchers' access to data, including datasets with deleted accounts and content, with a view to examining the influence of strategic disinformation on democratic decision making and on electoral processes, and possibly proposing the setting up of a European network of researchers in this area; g) considering national and international regulation to share best practices and increase co-operation among security agencies, for instance by creating a specific mechanism for monitoring, crisis management and post-crisis analysis and sharing resources that already exist in various countries, in line with Recommendation 2144 (2019) on

internet governance and human rights; h) calling on professionals and organizations in the media sector to develop self-regulation frameworks that contain professional and ethical standards relating to their coverage of election campaigns, including enhanced news accuracy and reliability and respect for human dignity and the principle of non-discrimination, in line with Resolution 2254 (2019); i) initiating judicial reforms and setting up specialized divisions for judges and prosecutors focusing on disinformation and hate speech[42].

An analysis of the recommendations of the Parliamentary Assembly of the Council of Europe shows that the Council of Europe recognizes the dangers of disinformation on the Internet and is looking for ways to counter this phenomenon. This creates a direct threat to the realization of the freedom of speech, as protected in the international system of human rights protection. The proposed activities are comprehensive. Much attention is paid to the educational effort, but also specification of legal instruments that should be implemented by the Member States is taking place. By emphasizing the importance of national and international regulations, where the Council of Europe is an active entity that creates, this organization also takes into account the importance of self-regulation in individual environments. They can be a valuable supplement to the instruments offered by state authorities in the form of statutory regulations and by international organizations in the form of multilateral agreements.

5. FINAL COMMENT

The phenomenon of information pollution begins to have increasingly significant negative effects on modern societies. Disinformation on the Internet and in other new media affects a number of areas of social life, and has recently become an important factor disrupting political life[43]. Several fundamental problems are involved due to important questions about the influence of "fake news", "disinformation order", "post-truth politics",

[42] Ibidem, § 6.

[43] Bruce Bimber and Homero Gil de Zúñiga, "The unedited public sphere," *New Media and Society* 22(4) (2020): 700–715.

"information smog" or "information pollution", to public and individuals lives. Global problems need new tactics and alliances like never before, because information pollution also has gone global[44]. They are followed by compulsion and demands how to resolve more and more strict plot of the new technologies expansion and the need to protect several individual and social values. The new approach to recognize new strategies, including strategic coalitions and constructing new frames for the available activities, is fundamental. The efforts of the Council of Europe to counteract these negative phenomena that threaten the realization of fundamental human rights are also more comprehensive than ever. They include the activities of the Committee of Ministers and other intergovernmental cooperation bodies, as well as the Parliamentary Assembly, based on the European Convention on Human Rights and the development of its provisions, especially worked out by the European Court of Human Rights. One cannot, however, disregard the so-called "soft law", offered, *inter alia*, by the Commission for Democracy through Law (Venice Commission). But the governance processes should be more broad and complete, including partners from ICT and media sectors, as well as another pan-European organizations, like the European Union, which perceives disinformation as a major challenge for Europe[45].

The recommendations of the Parliamentary Assembly of the Council of Europe analyzed are precisely "soft law". Although they are not legally binding in terms of public international law, they should nevertheless play an important role in directing the activity of Council of Europe member states. After all, the Council of Europe is called an "organization of values" and everything it offers serves to strengthen democracy, the rule of law and protect human rights. This effort, in conjunction with the activities of other international organizations, both universal (e.g. the United Nations) and regional (e.g. the European Union, OSCE) deserve support, regardless of the legal nature of the actions taken.

[44] Mark Scott, "POLITICO Digital Bridge: COVID-19 disinformation – Digital divide-Mark Warner," March 11, 2021, https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-covid-19-disinformation-digital-divide-mark-warner/, accessed March 22, 2021.

[45] Alicja Jaskiernia, "Europejska walka z dezinformacjami i nielegalnymi treściami w sieci. Obrona jakości mediów w Unii Europejskiej i Radzie Europy," *Studia Medioznawcze* 4(79) (2019): 384–394.

REFERENCES

Ahmed, Mohiuddin, Abu S. S. M. Barkat Ullah, and Al-Sakib Khan Pathan, eds. *Security analytics for the internet of everything*. Boca Raton, Florida, London, New York: CRC Press, 2020.

Asensio, Pedro de Miguel. *Conflict of laws and the internet*. Cheltenham, England, Northampton, Massachusetts: Edward Elgar Publishing, 2020.

Balas, Valentina E., Vijender Kumar Solanki, and Raghvendra Kumar, eds. *Internet of Things and Big Data Applications Recent Advances and Challenges*. Cham: Springer International Publishing, 2020.

Ball, James. *The system: who owns the internet, and how it owns us*. London: Bloomsbury Publishing, 2020.

Bimber, Bruce, and Homero Gil de Zúñiga. "The unedited public sphere." *New Media and Society* 22(4) (2020): 700–715.

Council of Europe Report on Information and Disorder. Strasbourg: Council of Europe, 2017.

DeNardis, Laura. *The Internet in Everything: Freedom and Security in a World with No Off Switch*. New Haven, CT: Yale University Press, 2020.

Denisova, Anastasia. *Internet memes and society: social, cultural, and political contexts*. New York, London: Routledge, 2019.

Deuze, Mark. "The Role of Media and Mass Communication Theory in the Global Pandemic." *Communication Today* 11, no. 2 (2020): 4–15.

Edwards, Lilian. *Law, policy and the Internet*. Oxford: Hart, 2019.

Fürnkranz, Gösta. *The Quantum Internet Ultrafast and Safe from Hackers*. Cham: Springer International Publishing, 2020.

Jaskiernia, Alicja. "Europejska walka z dezinformacjami i nielegalnymi treściami w sieci. Obrona jakości mediów w Unii Europejskiej i Radzie Europy." *Studia Medioznawcze* 4(79) (2019): 384–394.

Jung, Bohdan, and Tadeusz Kowalski. "Restructuring Time Use Under COVID-19 Pandemics." *International Journal of Inspiration & Resilience Economy* 5(1) (2021): 22–31.

McCulloch, Gretchen. *Because internet: understanding the new rules of language*. New York: Riverhead Books, 2019.

Meel, Priyanka, and Dinesh Kumar Vishvakarma. "Fake news, rumor, information pollution in social media and web: A contemporary survey of state-of-the-arts, challenges and opportunities." *Expert Systems with Applications* 153 (2020): 112986.

Meel, Priyanka, and Dinesh Kumar Vishwakarma. "A temporal ensembling based semi-supervised ConvNet for the detection of fake news articles." *Expert Systems with Applications* 177 (2021): 115002.

Moura, Vicente Dário, and Sofia de Vasconcelos Casimiro, eds. *Data Protection in the Internet*. Cham: Springer International Publishing, 2020.

Nielsen, Jakob. "IM, Not IP (Information Pollution): A steady dose of realtime interruptions is toxic to anyone's health." November 2003, Association for ComputingMachinery.https://dl.acm.org/doi/pdf/10.1145/966712.966731. Accessed March 23, 2021.

Orman, Levent. "Fighting Information Pollution with Decision Support Systems." *Journal of Management Information Systems* 1, no. 2 (2015): 64–71.

Reed, Thomas Vernon. *Digitized lives: culture, power, and social change in the internet era*. New York: Routledge, 2019.

Rohokale, Vandana. *Cyber Security: The Lifeline of Information and Communication Technology*. Cham: Springer International Publishing, 2020.

Scott, Mark. "POLITICO Digital Bridge: COVID-19 disinformation – Digital divide - Mark Warner." March 11, 2021. https://www.politico.eu/newsletter/digital-bridge/politico-digital-bridge-covid-19-disinformation-digital-divide-mark-warner/. Accessed March 22, 2021.

Shackelford, Scott J. *The Internet of Things: What Everyone Needs to Know*. New York: Oxford University Press, 2020.

Smith, Graham, Ruth Boardman, Flynn Cathal, and Gabe Maldoff. *Internet law and regulation*. London: Sweet & Maxwell, 2020.

Soro, Alessandro, Margot Brereton, and Paul Roe, eds. *Social Internet of Things*. Cham: Springer International Publishing, 2019.

Susi, Susi, ed. *Cyber Security: The Lifeline of Information and Communication Technology*. London, New York: Routledge, Taylor & Francis Group, 2019.

Synodinou, Tatiana-Eleni, Philippe Jougleux, Christiana Markou, and Thalia Prastitou, eds. *EU Internet Law in the Digital Era Regulation and Enforcement*. Cham: Springer International Publishing, 2020.