ISSN: 2957-2150

Czasopismo krajowego rejestru domen

Vol. I /2025

SPIS TREŚCI

Wstęp

Internet stał się jedną z podstawowych przestrzeni organizujących współczesne życie społeczne, ekonomiczne i polityczne. Nie jest on już wyłącznie narzędziem komunikacji, lecz środowiskiem, w którym kształtują się relacje społeczne, tożsamości jednostek, mechanizmy wpływu oraz nowe formy władzy. Z tego względu Internet stanowi dziś przedmiot równoczesnego zainteresowania wielu dyscyplin naukowych. Jest to przestrzeń zarówno regulacji normatywnej, jak i obszar dynamicznych procesów społecznych, które wymykają się tradycyjnym kategoriom.

Rozwój platform internetowych, mediów społecznościowych oraz systemów opartych na sztucznej inteligencji doprowadził do głębokiej transformacji sposobów komunikowania się, pozyskiwania informacji i uczestnictwa w sferze publicznej. Algorytmizacja przekazu, personalizacja treści oraz ekonomia uwagi wpływają na strukturę debaty publicznej, sprzyjając zarówno nowym formom partycypacji, jak i zjawiskom dezinformacji, polaryzacji oraz manipulacji informacyjnej. W konsekwencji prawo staje wobec wyzwania regulowania nie tylko infrastruktury Internetu, lecz także społecznych skutków jego funkcjonowania, w tym relacji władzy pomiędzy państwem, podmiotami prywatnymi i użytkownikami sieci.

Niniejszy numer czasopisma *dot.pl* podejmuje próbę interdyscyplinarnej analizy Internetu jako przestrzeni społecznie konstruowanej i prawnie regulowanej. Zaprezentowane artykuły ukazują, w jaki sposób technologie cyfrowe wpływają na procesy socjalizacji, formowanie opinii publicznej oraz redefinicję granic prywatności i autonomii jednostki. Szczególne miejsce zajmują rozważania dotyczące roli sztucznej inteligencji w komunikacji internetowej, w tym jej znaczenia dla rozpowszechniania teorii spiskowych, kształtowania narracji politycznych oraz utrwalania asymetrii informacyjnych.

Równocześnie autorzy podejmują zagadnienia związane z bezpieczeństwem Internetu i jego wykorzystywaniem jako narzędzia oddziaływania

politycznego oraz społecznego. Analizy konfliktów hybrydowych, „sharp power", państwowego nadzoru oraz cyfrowej dyplomacji wskazują, że Internet stał się istotnym polem rywalizacji państw i aktorów pozapaństwowych. Rodzi to pytania o legitymizację władzy, zakres dopuszczalnej kontroli oraz społeczną akceptację dla działań podejmowanych w imię bezpieczeństwa.

Istotnym wątkiem numeru są również regulacje prawne odnoszące się do funkcjonowania Internetu, w tym normy z zakresu cyberbezpieczeństwa, ochrony danych oraz treści cyfrowych. Analiza dyrektywy NIS 2 oraz zagadnień związanych z ochroną własności intelektualnej w sieci ukazuje napięcie pomiędzy potrzebą stabilności i ochrony porządku prawnego a dynamiką praktyk społecznych użytkowników Internetu. Prawo, aby zachować skuteczność, musi uwzględniać społeczne uwarunkowania technologii, a jednocześnie wyznaczać ramy odpowiedzialnego korzystania z cyfrowej przestrzeni.

Zgromadzone w niniejszym numerze artykuły potwierdzają, że Internet jako zjawisko społeczno-prawne wymaga pogłębionej refleksji interdyscyplinarnej. Połączenie wielu perspektyw pozwala nie tylko lepiej zrozumieć mechanizmy funkcjonowania świata cyfrowego, lecz także formułować bardziej adekwatne i społecznie osadzone rozwiązania regulacyjne. W tym sensie niniejszy numer *dot.pl* stanowi istotny głos w debacie nad przyszłością Internetu jako przestrzeni wolności, kontroli i odpowiedzialności.

Prof. dr hab. Katarzyna Chałubińska-Jentkiewicz
Dr hab. Urszula Soler
Redaktorki Naczelne

„dot.pl" - czasopismo Rejestru domeny .pl

From Online Media-World Socialization to the AI-Connected Society An Introduction to the Sociology of Communication and the New Challenges of AI

Nicola Strizzolo
University of Teramo, Department of Political Science, Italy
ORCID: https://orcid.org/0000-0001-6384-9210
E-mail: nstrizzolo@unite.it

Abstract

This article aims to propose an explanatory metaphor to describe the relationship of the Sociology of Communication with other branches of sociology, with society as a whole, and with the changes affecting both its objects of study and its core concepts – from the early mass societies, through the Internet age, and into the current era of Artificial Intelligence: the Sociological Cell.

At the center of this cell lie the fundamental and shared theories, methods, and objectives of the discipline; within the cytoplasm takes place the interaction among different sociological areas; and the various membranes ensure a semi-permeable exchange, both internal and external, safeguarding at once the identity of the discipline and its interdisciplinary vocation.

Received: 09.06.2025
Accepted: 02.07.2024
Published: 02.07.2024

Cite this article as:
N. Strizzolo, "*From Online Media-World Socialization to the AI-Connected Society An Introduction to the Sociology of Communication and the New Challenges of AI*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/207840

Corresponding author:
Nicola Strizzolo, University of Teramo, Department of Political Science , Italy
E-mail: nstrizzolo@unite.it

The article also outlines the challenges and topics the discipline has faced – and will have to face –as it evolves within an interconnected society shaped by a new triad: nature, culture, and the artificial.

Keywords: Sociology of Communication, Artificial Intelligence (AI), Connected and Online Society, Surveillance Capitalism, Digital Proletarianization

Introduction: The Sociology Cell

There have been numerous occasions where I have been called upon to introduce my academic field: the Sociology of Communication.

The proposed model is based on an organicistic vision which, however, does not seek to revive the positivist or functionalist theories of the discipline's early stages. Rather, it adopts the metaphor of a cell –*the Sociology Cell* –as a heuristic device, characterized by internal balances and exchanges with the external environment.

At its core – the nucleus, which in biology contains the genetic material and thus the identity and transmissive capacity of the cell –are located the fundamental components of the discipline: core theories, methods of inquiry, and shared objectives such as the understanding of social phenomena and the analysis of structures and relational dynamics.

The cytoplasm, the intracellular fluid where vital reactions occur and where organelles operate –specialized structures responsible for energy production or protein synthesis – symbolizes, in this metaphor, the context of interaction among the various branches of sociology. Here, the circulation and mutual fertilization of ideas take place through a form of theoretical and conceptual osmosis, ensuring dialogic density and an interdisciplinary orientation[1].

The internal membranes of the cell, which in biological systems compartmentalize specific functions (such as in mitochondria or the endoplasmic reticulum), correspond to the various subfields of sociology, which remain in communication with one another –

[1] E. Morin, *Introduction à la pensée complexe*, ESF Éditeur, Paris 1990.

listed here without claiming exhaustiveness: general sociology; sociology of cultural and communicative processes; legal and deviance sociology; family, religion, gender, territorial, political, educational, migration, and social change sociology.

The outer membrane of the cell, which in biology preserves the integrity and cohesion of the system while being semipermeable, parallels sociology's capacity to remain open to external contributions –from other social sciences, cognitive sciences, and philosophy, to public and political communication –while also engaging with society at large through the perspective of sociologists who are both immersed in their time and equipped with theoretical and methodological tools.

Within this framework, the need for a dialogical relationship with public and institutional communication becomes evident[2], as does the importance of a critical reflection on digital transformation[3].

In biology, homeostasis refers to the way a cell maintains internal balance by regulating conditions through controlled exchanges –like the turgor pressure in plant tissues. There is, in fact, an internal "pressure and density" within the various areas of sociology, which may lead them to seek recognition, or conversely, to lose it –merging into related fields or absorbing them.

Adaptation, by contrast, allows for innovative responses to change: it is essential for survival and for the transmission of evolutionary advantages.

Sociology shows its vitality in a similar way: by adjusting its interpretive models in response to shifts in culture, technology, and global dynamics – from the rise of digital systems to the emergence of complex, systemic challenges.

Topics in the Sociology of Communication

The sociology of communication, which investigates diverse audiences and media usage in connection with broader social and cultural developments –in other words, in a state of interdependence – embodies the very mechanism of correspondence between the evolution of society, the 'Sociology Cell,' and its internal components.

---

[2] A. Lovari, G. Ducci, *Comunicazione pubblica. Istituzioni, pratiche, piattaforme*, Mondadori Università, Milano 2022.

[3] N. Strizzolo et al., *La comunicazione eclettica. Le dimensioni comunicative nella web society*, FrancoAngeli, Milano 2020.

At least three major transformative phases can be identified:

1. The emergence of mass society, shaped by the early mass media and oriented toward consumption. The rise of modern media is closely tied to industrialization, national-popular culture, and the formation of a large audience, conceived as passive and homogeneous.
2. The spread of media –initially analog and later digital –has led to the development of an interconnected society. Within social media environments, we have witnessed an accelerated shift from 'community' to online 'society.[4]'
3. The blurring of the boundary between producer and consumer, together with the process of datafication, has ushered in the age of surveillance capitalism, marked by a condition of algorithmic proletarianization.

In the first phase, we witness the rise of industrialization, which drove the migration from rural areas to metropolitan centers, the spread of rational bureaucracy to manage them[5], the disenchantment of the world[6], and eventually, its globalization[7].

Early media, supported not only by advances in electronics but also by the creation of global communication channels – under the seas and above the skies[8] – effectively eliminated distance and gave rise to a new kind of village on a global scale[9]. In doing so, they first neutralized the very sense of spatiality[10], and later that of 'places' –temples and theatres of consumption, entertainment, and transience[11].

In the second phase, an accelerated movement toward various forms of convergence unfolds: digital technology increasingly integrates different cultural domains and

[4] Ibidem.
[5] M. Weber, *Economy and Society: An Outline of Interpretive Sociology*, University of California Press, Berkeley 1978.
[6] M. Weber, *La scienza come professione. Il lavoro intellettuale come professione*, Einaudi, Torino 1966.
[7] A. Giddens, *The Consequences of Modernity*, Stanford University Press, Stanford 1990.
[8] A. Mattelart, *L'invenzione della comunicazione*, Il Saggiatore, Milano 1998.
[9] M. McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man*, University of Toronto Press, Toronto 1962.
[10] J. Meyrowitz, *No Sense of Place: The Impact of Electronic Media on Social Behavior*, Oxford University Press, New York 1985.
[11] M. Augé, *Non-lieux. Introduction à une anthropologie de la surmodernité*, Seuil, Paris 1992; J. Urry, *Mobilities*, Polity Press, Cambridge 2007.

eventually connects diverse social moments, giving rise to a *platform society* or *social society*[12].

All of this occurs against the backdrop of a disintermediated system of media production and consumption, which has expanded the volume of information to the point of turning it into disinformation –an ecosystem now increasingly shaped by artificial actors as well[13].

Specifically, by *social society* I refer to a society that self-represents through media and networked systems that have enveloped the entire globe and permeated all spheres of life –no moment or activity remains untouched[14].

Within the neoliberal framework, where the consumer becomes both product and producer, a spiral of self-representation and self-consumption takes shape: those who have nothing else to offer – unlike the most followed celebrities, who are famous for achievements in sports, entertainment, or politics – offer increasingly vast and intense portions of themselves, hoping to monetize potential *likes*, effectively merging the performed persona with their entire lived existence[15].

This dynamic gives rise to a new form of proletarianization –what I define as '*algorithmic proletarianization*' – in which individuals from all walks of life, including parents who publicly expose their children with severe disabilities or people in conditions of extreme marginality, stage themselves and their families alongside improbable videos of performative acts or commentary – often lacking both expertise and coherence – on current events or content from the mainstream and subcultural media industries. Under *surveillance capitalism*, individuals "consume" themselves on social media even without producing content: the data generated by their activities –including passive browsing –are harvested by algorithms to fuel the surveillance economy[16].

---

[12] J. Van Dijck et al., *The Platform Society: Public Values in a Connective World*, Oxford University Press, Oxford 2018; N. Strizzolo et al., *La comunicazione eclettica. Le dimensioni comunicative nella web society*, FrancoAngeli, Milano 2020.

[13] N. Strizzolo et al., The Information Overload of Global Information Systems: More Information, Less Certainty; More Disinformation, Less Society, in K. Chałubińska-Jentkiewicz, U. Soler (Ed.), *Legal, Sociological and Political Aspects of Disinformation – Based on the Example of the Coronavirus Pandemic*, Adam Marszałek Publishing House, Toruń 2023, pp. 134–143.

[14] N. Strizzolo et al., C. Melchior, *La comunicazione eclettica. Le dimensioni comunicative nella web society*, FrancoAngeli, Milano 2020.

[15] A. Elliott, *Identity Troubles: An Introduction*, Routledge, London-New York 2013.

[16] S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York 2019.

All of this occurs within increasingly artificial environments, such as the metaverse, where digital horizons reshape the very coordinates of reality.

Disintermediation has fostered a horizontal culture and a non-hierarchical system of knowledge organization, known as *folksonomy*[17]. However, the overabundance of information thus generated produces entropy rather than clarity.[18] A phenomenon that feeds into disinformation and post-truth: fake news proliferates, and cognitive stress caused by information overload –along with the constant need to assess the veracity of content –prevents clear identification of reliable sources[19].

A pervasive distrust emerges, fueled both by continuous transparency regarding scandals across various domains –not only media-related –and by the parallel spread of conspiracy theories. This widespread suspicion further erodes social capital[20], culminating in a scenario of isolated individuals, in a state of permanent vigilance, as if under siege - surrounded by threats, dangers, and fears - closely resembling the "minimal self" described by Lasch[21].

These are artificial – not merely virtual - situations, in which physical environments themselves are no longer designed on a human scale, but are instead shaped to optimize technological functioning[22].

In this new world, AI emerges as a *parasocial actor*, capable of managing communication flows that human operators cannot handle; it generates both authentic and false content; and it influences institutional, social, and political communication processes.

This scenario potentially ushers in a new crisis of democratic communication, manifested through:

[17] T. Vander Wal, Folksonomy Coinage and Definition, 2007. https://vanderwal.net/folksonomy.html

[18] N. Strizzolo et al., The Information Overload of Global Information Systems: More Information, Less Certainty; More Disinformation, Less Society, in K. Chałubińska-Jentkiewicz, U. Soler (Ed.), *Legal, Sociological and Political Aspects of Disinformation – Based on the Example of the Coronavirus Pandemic*, Adam Marszałek Publishing House, Toruń 2023, pp. 134–143.

[19] Ibidem.

[20] R. D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, Simon & Schuster, New York 2000.

[21] C. Lasch, *The Minimal Self: Psychic Survival in Troubled Times*, Norton, New York 1984.

[22] L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, a cura di M. Durante, Raffaello Cortina Editore, Milano 2022.

- manipulation carried out by bots, algorithms, and machine learning systems, leading to the loss of control by individuals and institutions over communicative flows;
- concerns about transparency, at risk both in how algorithms operate and in the content they produce;
- renewed issues of trust - this time, in relation to the actions and outputs of AI systems.

Finally, as human agency becomes diminished or marginalized – given the vast range of tasks now performed by machines, the density of information, and the velocity of socially induced change – communication appears to have taken center stage as a media performance detached from any grounding in factual truth.

A dystopian realization of the concept of *media-world*[23]: digital and Internet-based media now create an environment with increasingly blurred boundaries between physical and virtual reality. Media have become integral to the human experience, shaping perception, social relationships, and cultural processes. Today, this includes AI.

We are well beyond *com-fusion*[24] – the seamless fusion between participatory relationships and online actions. Currently, cognitive and cultural interactions are increasingly mediated by machines: AI systems, having exhausted the supply of human data available on the web, are beginning to autonomously generate new content.

Even the traditional themes of sociology of communication – such as socialization, manipulation, or identity – have been profoundly redefined by the rise of Internet-based platforms and the expansion of online ecosystems, which have reshaped relational dynamics, access to information, and modes of expression.

In this new scenario, numerous key research areas of the sociology of communication come into play, including:

- Socialization, initially understood as the influence of audiovisual content on processes of personality development[25];

[23] G. Boccia Artieri, *I media-mondo. Forme e linguaggi dell'esperienza contemporanea*, Meltemi, Roma 2004.
[24] N. Strizzolo, *Com-fusion: Fusion between on-line and off-line through communicative interaction*, in *Conference Tales of the Unexpected. Vision and Reality in Community Informatics*, pp. 1–8, Monash Centre 2010.
[25] S. Martelli, *Videosocializzazione: Processi educativi e nuovi media*, FrancoAngeli, Milano 2001.

- Technology and society, particularly the relationship between media environments and social structures[26];
- Influence and manipulation, through the study of persuasive strategies, propaganda techniques, and rhetorical devices employed by the media[27];
- Digital inclusion, with specific attention to the digital divide as a form of exclusion from access to resources, knowledge, and civic participation[28];
- Equality and inequality, examined through the media's effectiveness in fostering awareness and shaping social representations, drawing on theoretical models such as framing and newsmaking[29];
- Interpersonal relationships, both among online users and between lived identities and their digital self-representations[30];
- Gender and sexuality, focusing on the media's role in constructing roles, stereotypes, and orientations[31];
- Sustainability and ethics, at the intersection of communication, environmental awareness, and social responsibility[32];
- Sports and media, with emphasis on spectacularization, identity formation, and new bodily languages[33];
- Health, from the perspectives of public communication, prevention, medicalization, and citizen participation[34];

[26] F. Colombo, *Il potere socievole. Storia e critica dei social media*, Bruno Mondadori, Milano 2013.
[27] G. Gili, *Il problema della manipolazione: peccato originale dei media?*, FrancoAngeli, Milano 2001.
[28] S. Bentivegna, *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Laterza, Roma-Bari 2009.
[29] D. E. Kendall, *Framing Class: Media Representations of Wealth and Poverty in America*, Rowman & Littlefield, Lanham 2005; V. Fielding, *Media Inequality: News Framing and Media Power*, Routledge, Abingdon 2025.
[30] G. Boccia Artieri et al., *Fenomenologia dei social network. Presenza, relazioni e consumi mediali degli italiani online*, Guerini Scientifica, Milano 2017.
[31] M. Farci et al., *Media digitali, genere e sessualità*, Mondadori Università, Milano 2022.
[32] F. Colombo, *Ecologia dei media. Manifesto per una comunicazione gentile*, Vita e Pensiero, Milano 2020.
[33] L. Bifulco et al., *Sport e scienze sociali. Fenomeni sportivi tra consumi, media e processi globali*, Rogas Edizioni, Roma 2019.
[34] E. Gola et al., *Comunicare la salute. Metodi e buone pratiche per le amministrazioni pubbliche*, Carocci, Roma 2018.

- Politics, with particular attention to the construction of public discourse, representation, and digital citizenship[35].

Today, we find ourselves in a scenario where artificial intelligence is increasingly pervasive - sometimes as an ambient constant, other times as a determining variable[36]. AI contributes not only to everyday applications across all spheres of life, but also to a redefinition of the very concept of the *social body*, which is now being constructed in symbiosis with algorithmic systems[37] (Floridi, 2022).

This is particularly evident in the domain of health and embodiment, where human corporeality is increasingly integrated with technological support[38], but it also extends to AI's involvement in processes of cultural mediation and production[39].

Artificial intelligence is no longer merely a technical tool but a *cultural actor*: it generates content for the culture industry and, in some cases, contributes to the construction of symbolic imaginaries – including spiritual ones[40]. This does not refer solely to transhumanist debates, but also to the creation of symbolic elements that enter the realm of the sacred, such as the automated generation of prayers, symbols, or even homilies.

Conclusion: Returning to the Cell

Returning to the metaphor of the sociology cell, the sociology of communication today performs the specific function of analyzing the communicative flows that traverse society, in close connection with the sociology of cultural processes.

---

[35] M. Sorice, *I media e la democrazia*, Carocci, Roma 2014; A. Lovari, G. Ducci, *Comunicazione pubblica. Istituzioni, pratiche, piattaforme*, Mondadori Università, Milano 2022.
[36] K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven 2021.
[37] L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, a cura di M. Durante, Raffaello Cortina Editore, Milano 2022.
[38] World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*, World Health Organization, Geneva 2021. https://apps.who.int/iris/handle/10665/341996
[39] K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven 2021; R. Schäfer, S. Biderman, C. Raffel, N. Shazeer, M. Welling, The Curse of Recursion: Training on Generated Data Makes Models Forget, *arXiv*, 2024. https://doi.org/10.48550/arXiv.2305.17493
[40] AI Research Group of the Centre for Digital Culture, Encountering Artificial Intelligence: Ethical and Anthropological Investigations, "Journal of Moral Theology", 1 (Theological Investigations of AI), pp–262, 2023.

It represents a “complementary organ,” essential for understanding how communicative content both influences and is influenced by culture. However, this relationship is now evolving: from the traditional nature–culture binary to a triadic framework of nature-culture-artificial.

In light of these transformations, the study of the connected and artificial society becomes central. The very boundaries of the sociology of communication – as well as those of other sociological domains – are being reconfigured to address new epistemological challenges, renewed analytical demands, and emerging methodological possibilities.

References

AI Research Group of the Centre for Digital Culture, Encountering Artificial Intelligence: Ethical and Anthropological Investigations, “Journal of Moral Theology”, 1 (Theological Investigations of AI): i–262, 2023.

M. Augé, *Non-lieux. Introduction à une anthropologie de la surmodernité*, Seuil, Paris 1992.

S. Bentivegna, *Disuguaglianze digitali. Le nuove forme di esclusione nella società dell'informazione*, Laterza, Roma-Bari 2009.

L. Bifulco, M. Tirino (a cura di), *Sport e scienze sociali. Fenomeni sportivi tra consumi, media e processi globali*, Rogas Edizioni, Roma 2019.

G. Boccia Artieri, *I media-mondo. Forme e linguaggi dell'esperienza contemporanea*, Meltemi, Roma 2004.

G. Boccia Artieri, L. Gemini, F. Pasquali, S. Carlo, M. Farci, M. Pedroni, *Fenomenologia dei social network. Presenza, relazioni e consumi mediali degli italiani online*, Guerini Scientifica, Milano 2017.

A. Bruns, *Blogs, Wikipedia, Second Life, and Beyond: From Production to Produsage*, Peter Lang, New York 2008.

M. Castells, *The Rise of the Network Society*, Blackwell, Oxford 1996.

V. Codeluppi, *Mi metto in vetrina. Selfie, Facebook, Apple, Hello Kitty, Renzi e altre «vetrinizzazioni»*, Mimesis, Milano-Udine 2015.

F. Colombo, *Il potere socievole. Storia e critica dei social media*, Bruno Mondadori, Milano 2013.

F. Colombo, *Ecologia dei media. Manifesto per una comunicazione gentile*, Vita e Pensiero, Milano 2020.

K. Crawford, *Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*, Yale University Press, New Haven 2021.

G. Debord, *La société du spectacle*, Buchet-Chastel, Paris 1967.

P. De Salvo, M. Pizzi, *Narrazione, sviluppo e governo del territorio. Un percorso fra identità, turismo, partecipazione e competizione*, FrancoAngeli, Milano 2023.

M. Farci, C. M. Scarcelli (a cura di), *Media digitali, genere e sessualità*, Mondadori Università, Milano 2022.

V. Fielding, *Media Inequality: News Framing and Media Power*, Routledge, Abingdon 2025.

L. Floridi, *Etica dell'intelligenza artificiale. Sviluppi, opportunità, sfide*, a cura di M. Durante, Raffaello Cortina Editore, Milano 2022.

A. Giddens, *The Consequences of Modernity*, Stanford University Press, Stanford 1990.

G. Gili, *Il problema della manipolazione: peccato originale dei media?*, FrancoAngeli, Milano 2001.

E. Gola, F. Meloni, R. Porcu, *Comunicare la salute. Metodi e buone pratiche per le amministrazioni pubbliche*, Carocci, Roma 2018.

D. E. Kendall, *Framing Class: Media Representations of Wealth and Poverty in America*, Rowman & Littlefield, Lanham 2005.

A. Lovari, G. Ducci, *Comunicazione pubblica. Istituzioni, pratiche, piattaforme*, Mondadori Università, Milano 2022.

S. Martelli (a cura di), *Videosocializzazione: Processi educativi e nuovi media*, FrancoAngeli, Milano 2001.

A. Mattelart, *L'invenzione della comunicazione*, trad. it. di G. Salinas, Il Saggiatore, Milano 1998.
V. Mayer-Schönberger, K. Cukier, *Big Data: A Revolution That Will Transform How We Live, Work, and Think*, Houghton Mifflin Harcourt, Boston 2013.
M. McLuhan, *The Gutenberg Galaxy: The Making of Typographic Man*, University of Toronto Press, Toronto 1962.
M. McLuhan, *Understanding Media: The Extensions of Man*, McGraw-Hill, New York 1964.
J. Meyrowitz, *No Sense of Place: The Impact of Electronic Media on Social Behavior*, Oxford University Press, New York 1985.
E. Morin, *L'esprit du temps. Essai sur la culture de masse*, Seuil, Paris 1962.
E. Morin, *Introduction à la pensée complexe*, ESF Éditeur, Paris 1990.
G. Pietropolli Charmet, *L'insostenibile bisogno di ammirazione*, Laterza, Roma-Bari 2019.
R. D. Putnam, *Bowling Alone: The Collapse and Revival of American Community*, Simon & Schuster, New York 2000.
R. Schäfer, S. Biderman, C. Raffel, N. Shazeer, M. Welling, The Curse of Recursion: Training on Generated Data Makes Models Forget, *arXiv*, 2024. https://doi.org/10.48550/arXiv.2305.17493
M. Sorice, *I media e la democrazia*, Carocci, Roma 2014.
N. Strizzolo, *Com-fusion: Fusion between on-line and off-line through communicative interaction*, in *Conference Tales of the Unexpected. Vision and Reality in Community Informatics*, pp. 1–8, Monash Centre 2010.
N. Strizzolo, G. Cossi, The Information Overload of Global Information Systems: More Information, Less Certainty; More Disinformation, Less Society, in K. Chałubińska-Jentkiewicz, U. Soler (Ed.), *Legal, Sociological and Political Aspects of Disinformation – Based on the Example of the Coronavirus Pandemic*, Adam Marszałek Publishing House, Toruń 2023, pp. 134–143.
N. Strizzolo, A. Pocecco, C. Melchior, *La comunicazione eclettica. Le dimensioni comunicative nella web society*, FrancoAngeli, Milano 2020.
N. Taleb, *The Black Swan: The Impact of the Highly Improbable*, Random House, New York 2007.
J. Van Dijck, T. Poell, M. de Waal, *The Platform Society: Public Values in a Connective World*, Oxford University Press, Oxford 2018.
T. Vander Wal, Folksonomy Coinage and Definition, 2007. https://vanderwal.net/folksonomy.html
M. Weber, *La scienza come professione. Il lavoro intellettuale come professione*, Einaudi, Torino 1966.
M. Weber, *Economy and Society: An Outline of Interpretive Sociology*, a cura di G. Roth e C. Wittich, University of California Press, Berkeley 1978.
World Health Organization, *Ethics and Governance of Artificial Intelligence for Health: WHO Guidance*, World Health Organization, Geneva 2021. https://apps.who.int/iris/handle/10665/341996
S. Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*, PublicAffairs, New York 2019.
J. Urry, *Mobilities*, Polity Press, Cambridge 2007.

„dot.pl" - czasopismo Rejestru domeny .pl

Using Critical Realism to analyse Big Data: ontic, epistemic, and ethical assumptions

Małgorzata Stochmal
University of Wroclaw, Faculty of Social Sciences, Poland
ORCID: https://orcid.org/0000-0002-8385-2844
E-mail: malgorzata.stochmal@uwr.edu.pl

Abstract

Critical realism remains an interesting research program to explore social reality in an in-depth way. A reflection on its creation is intended to alleviate the shortcomings of positivist and post-positivist approaches. The main aim of the article is to present the ontological, epistemological and ethical assumptions of critical realism. These assumptions can be successfully applied when implementing analytical projects related to large data sets. The article is addressed to recipients interested in a critical and realistic vision of the description of reality related to broadly understood big data analytics.

Keywords: Big Data, stratified depth of ontology, the depth of epistemology, Critical realism, transcendent reality

Received: 15.07.2025
Accepted: 07.08.2025
Published: 07.08.2025

Cite this article as:
M. Stochmal, "Using Critical Realism to analyse Big Data: ontic, epistemic, and ethical assumptions"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/209115

Corresponding author:
Małgorzata Stochmal
University of Wroclaw, Faculty of Social Sciences, Poland

E-mail:
malgorzata.stochmal@uwr.edu.pl

Introduction

The expansion of human activity in the digital sphere is accelerating, with no signs that its significance will diminish in the foreseeable future. Enthusiasts of Big Data argue that this phenomenon marks a civilizational breakthrough, comparable to the invention of the Internet, the steam engine, or the printing press[1]. We have progressed from storing kilobytes on floppy disks, to megabytes on hard drives, terabytes on disk arrays, and now petabytes in the cloud.[2] This trajectory continues toward even greater volumes of data — zettabytes, yottabytes, and exabytes. Massive data archives are being created to meet the growing demand for digital storage. Many events and interactions that once took place solely in the physical world now occur in digital spaces. As innovative technologies evolve, algorithms — due to the scale of analysis and the complexity of decision-making — not only mediate digital interactions but increasingly shape or even determine the decision-making process itself[3]. Equally striking is the transition from traditional social research to large-scale data digital analytics. The scale and speed of this technological shift are remarkable.

This article aims to provide a metatheoretical reconstruction of the ontological, epistemological, and ethical assumptions of critical realism and to analyze their applicability within the Big Data environment, in response to the question of how these assumptions can be employed to investigate the complexity of digital social reality. The research problem takes the following form: How can the ontological, epistemological, and ethical assumptions of critical realism be applied to the analysis of data in Big Data environments, considering their complex structure and related epistemic and normative challenges?

The techniques currently used in social research are referred to as obsolete, which is associated with some kind of crisis in empirical sociology[4]. Is this really how this

[1] R. Żulicki, *Potencjał Big Data w badaniach społecznych*. „Studia Socjologiczne", 3(266)/2017, p. 175.
[2] Ch. Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, https://www.wired.com/2008/06/pb-theory/ accesed 31 october 2024.
[3] B. D. Mittelstadt et al., *The ethics of algorithms: Mapping the debate*, „Big Data & Society" 3(2) (2016), p. 2, DOI: 10.1177/2053951716679679.
[4] M. Savage, R. Burrows, *The coming crisis of empirical sociology*, „Sociology" 41(5)/2007, pp. 885–899, DOI: 10.1177/0038038507080443.

situation should be perceived? Definitely not, each type of research creates its own challenges and is conducted in a specific scientific paradigm with the use of adequate analytical techniques. It is true that the analysis of large data sets allows social researchers to delve deeper into the phenomena being explored in a way that is disproportionate to traditional research[5]. The view of reality changes due to the complexity and changeability of its accompanying conditions. We are currently witnessing the fourth paradigm; the individual stages are characterized as follows:

1. Experimental science. Empiricism; describing natural phenomena (pre-Renaissance).
2. Theoretical science. Modelling and generalization (pre-computers).
3. Computational science. Simulation of complex phenomena (pre-Big Data).
4. Exploratory science. Data-intensive; statistical exploration and data mining[6].

Critical realism can also provide the foundation for proper research design, from theoretical assumptions to the construction of the initial model, to the selection of data inputted for analysis, and by how to analyze it and determine the meanings of the results obtained.

The stratified depth of ontology

In critical realism, priority is given to ontology, which ranks above epistemology. Ontology deals with the existence of beings and strong assumptions about their nature. The form of a strongly rooted realistic ontology restores the proper place not only to being, but also to its absence. The fact that we do not perceive a being at some point is not a proof of its non-existence, but it may result from its absence conditioned by the external context. Ontology as a theory of being emphasizes that all beings located in social, cultural, natural, biological or psychological reality exist independently of our any - complete or incomplete, fallible or true — awareness of them. The fact that they exist forces the tacit assumption that they operate in a strictly defined manner (e.g. the law of gravity, gravity, social inequalities, etc.).

[5] K. Krzysztofek, *Big Data Society. Technologie samozapisu i samopokazu*, „Transformacje. Pismo interdyscyplinarne", 1–4(72–55)/2012, pp. 223–257.
[6] R. Kitchin, *Big Data, new epistemologies and paradigm shifts*, „Big Data & Society" 1(1)/2014, p. 3-6, DOI: 10.1177/2053951714528481.

The ontology of being has not been reduced to one dimension, but analyses its coherent structure in depth. Each being should be analyzed in a deathly way, revealing more and more precise characteristics located on its individual layers.

A stratified ontology contains three elements placed in relation to each other: *Domain of Empirical*, d*omain of Actual* and d*omain of Real* [7]. A visualization of this concept is presented in Diagram 1.

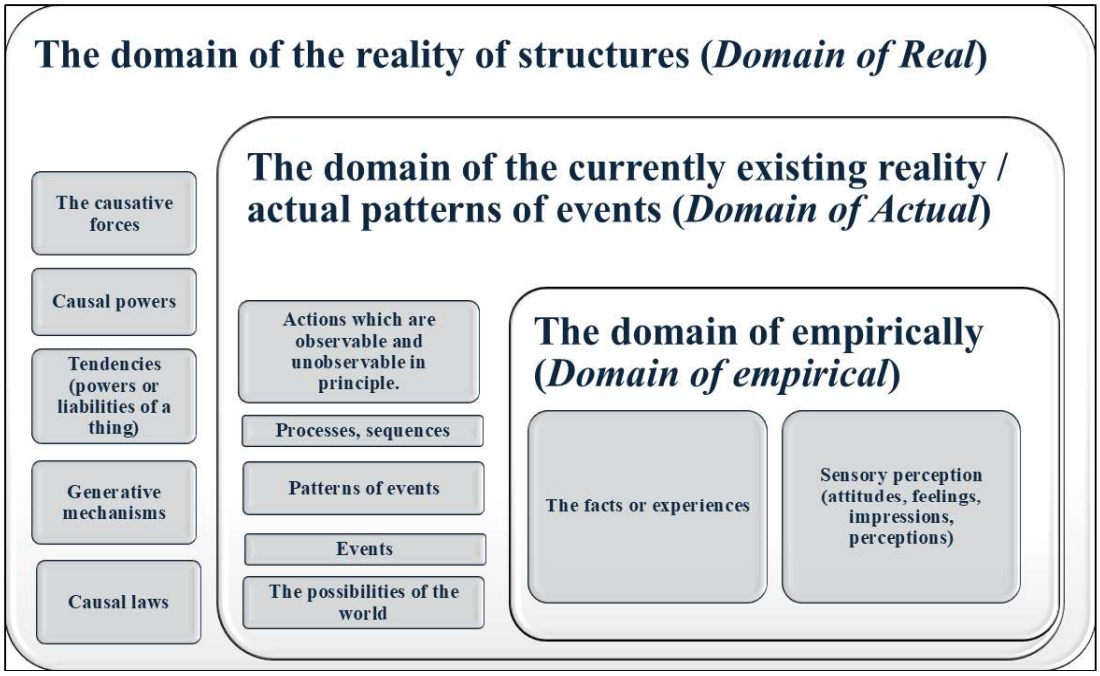


Diagram 1: *Ontological in-depth structures of reality in critical realism*
Source: Translated from M. Stochmal, Krytyczny realizm Roya Bhaskara – Basic Critical Realism, "Uniwersyteckie Czasopismo Socjologiczne", 31(1)/2023, p.12. https://doi.org/10.21697/ucs.2023.31.1.02

Roy Bhaskar proposed a stratified and differentiated model of reality that reveals the structured complexity of the ontological realm. According to his theory, reality consists of three analytically distinct but interrelated domains: the empirical, the actual, and the real. These domains are emergent, meaning that each arises from the conditions of the one beneath it while retaining a degree of relative autonomy. They are also temporally displaced, which is particularly significant in the context of scientific inquiry, as research is rarely conducted in real time but often retrospectively, based on empirical traces of past events.

[7] R. Bhaskar, *Enlightened Common Sense: The Philosophy of Critical Realism*, In Introduction Mervyn Hartwig, Pub. Routledge, Abingdon 2016, s. 6-7.

Bhaskar highlighted what he termed the "emergent powers of emergence"—the idea that new causal powers arise at higher levels of ontological complexity. The stratified ontology he proposed does not merely reflect the natural order in a linear fashion; rather, it captures the deep relationality and necessary co-existence of entities and mechanisms across levels of reality. This ontological depth aligns with the complex, layered nature of social and natural phenomena, making it a powerful framework for scientific explanation.

An important consideration, often overlooked in data-driven environments, is the potential mismatch between the purposes for which users generate or provide data and the purposes for which such data are subsequently collected, categorized, and analysed. From a critical realist perspective, this discrepancy underscores the ontological stratification of social reality: while users act within the empirical domain, expressing intentions or needs, the systems that process their input operate on assumptions situated at the actual or even the real domain. Recognizing this misalignment is essential for uncovering the generative mechanisms that underlie the data structures and for avoiding epistemic fallacies rooted in surface-level correlations.

Within this framework, the empirical domain constitutes the most immediately accessible level of reality—what is experienced through observation and sense perception. This includes *facts*, *events*, *sensations*, and *practices* as they appear to human consciousness. However, Bhaskar warns against empirical reductionism: the idea that what is experienced exhausts what is real. Experiences should not be taken as the sole basis for scientific generalization, but rather as the surface expressions of deeper mechanisms.

It is crucial to distinguish between what is *experienced* and what actually *occurs*. The world exists independently of our perception of it, and many events or mechanisms may remain unexperienced yet real. For instance, rainfall is a real event governed by causal mechanisms. However, due to space-time conditions, some people will experience it directly (by getting wet), while others will not—despite the event occurring in the same ontological reality. This example illustrates the transfactual nature of reality in critical realism: mechanisms can operate even when their effects are not empirically manifest.

The domain of the actual refers to the level of reality in which events and processes occur, regardless of whether they are experienced or observed. It occupies the intermediate stratum within Bhaskar's stratified ontology, situated between the domain of the real (generative mechanisms) and the domain of the empirical (experiences). The term "actual" is significant because it denotes the ontological status of events that have taken place or are taking place, independent of their empirical registration. Bhaskar himself states that "(t)he intelligibility of scientific change (and criticism) and scientific education thus presupposes the ontological independence of the objects of experience from the objects of which they are the experiences"[8]. This underscores the necessity of distinguishing between what exists and occurs and what is perceived or known.

Events in the actual domain are caused by real mechanisms, but they may or may not be empirically apprehended. This domain thus includes patterns of events, practices, and interactions that are shaped by underlying structures and mechanisms but are not reducible to immediate experience. It is within this domain that the conditions are set for empirical experience to be possible — including the availability of resources, conceptual frameworks, social practices, and relational contexts. While analytically distinct, the actual and empirical domains are causally linked: empirical observations are always contingent expressions of what has actually occurred, and both are grounded in the generative mechanisms located in the real domain. These events are situated at the middle level of the stratified ontology of reality. They comprise the conditions and configurations—including resources, concepts, practices, and relationships—that make experience in the empirical domain possible.

We thus arrive at the final layer - the domain of real structures, which constitutes the level at which generative mechanisms and causal laws emerge. These mechanisms produce phenomena that manifest as events in the actual domain and may be experienced empirically. Bhaskar defines the function of generative mechanisms as follows:

[8]R. Bhaskar, *A Realist Theory of Science*, with an Introduction by Mervyn Hartwig, Pub. Routledge, London and New York 2008, p. 21.

> “The real basis of causal laws are provided by the generative mechanisms of nature. Such generative mechanisms are, it is argued, nothing other than the ways of acting of things. And causal laws must be analysed as their tendencies. Tendencies may be regarded as powers or liabilities of a thing which may be exercised without being manifest in any particular outcome” (Bhaskar 2008:3)[9].

In the domain of real structures, causal forces are disclosed that activate the powers of generative mechanisms, which, in response to specific conditions, lead subjects to act in particular ways within the empirical domain. Generative mechanisms thus have the potential to produce events, which subsequently become manifest through perceived experience. These mechanisms generate event sequences that support the formulation of causal laws, expressing regularities observable under specific conditions.

While maintaining the ontological rigor of identifying entities embedded in social reality, this bottom-up and iterative process of determining their nature must be conducted carefully. However, the outcomes of such inquiry should not be distorted by the subjectivism of the researcher. The ontological depth structures of reality, as conceived in critical realism, may thus be described as a distinct form of ontological morphology.

Epistemic meanders

The domain in which scientific laws emerge is epistemology, understood as the sphere concerned with the generation and production of scientific knowledge. A central assumption of critical realism is epistemic relativism, which affirms the inherent fallibility of human knowledge and the historically and socially conditioned nature of the truths that individuals formulate.

“Epistemic realism means that all our claims are socially and historically conditioned. Our judgments are determined by circumstances, by what we know at the time and by binding criteria of judgment. For this reason, among other things, our judgments are always error prone. Epistemic relativism then means that each of us is in a situation from

[9]Ibidem, p. 3.

which we see the world in a slightly different way. Our experiences of the world are different”[10].

This fallibility arises from the spatio-temporal context in which knowledge is produced—it is generated at a specific historical moment and, over time, may be revised, distorted, or falsified. The social production of knowledge is burdened with factors that may unintentionally obscure or misrepresent the truth. Bhaskar characterizes science as "a process-in-motion", asserting that "knowledge must be viewed as the produced means of production, and science as a constant social activity in a continuous process of transformation." Furthermore, knowledge is always mediated by concepts, language, history, and social constructs that emerge within particular contexts. The production of knowledge takes place within open social systems, which are inherently dynamic and structurally contingent.

Alongside epistemic relativism and the recognition of ontological depth, attention must also be given to the rationality of judgments. This rationality pertains to the capacity to evaluate competing theoretical frameworks and to adopt the one that most adequately explains the phenomenon in question. Scientific knowledge advances through rational discourse, wherein scholars present evidence and engage in reasoned argumentation. The explanation that most convincingly accounts for the object of inquiry prevails. It must also be acknowledged that all knowledge production is, to some extent, mediated by the researcher’s perspective, their interpretation of reality, and their conceptual resources.

Bhaskar distinguishes between two fundamental dimensions of knowledge: the transitive and the intransitive. Transitive objects of knowledge serve as the initial means of production through which intransitive knowledge is formulated. The transitive dimension encompasses the raw materials of science—that is, conceptual and methodological constructs shaped by the prevailing scientific paradigms of a given historical moment. These are inherently changeable, reflecting the critical character of science as a self-transformative enterprise that occasionally yields breakthrough insights into the world. As Bhaskar explains: “Scientists try to discover the reasons for things and events, patterns and processes, sequences and structures. To understand how they do

[10]M. S. Archer, A. Collier, D. V. Porpora, *Transcendencja. Realizm krytyczny i Bóg*, trans. and Introduction Artur Wysocki, epilog Krzysztof Wielecki, Pub. UKSW, Warszawa 2021, p.55.

so one needs both a concept of the transitive process of knowledge-production and a concept of the intransitive objects of the knowledge they produce: the real mechanisms that generate the actual phenomena of the world, including as a special case our perceptions of them"[11].

Objects of transitory knowledge connect the adopted "facts and theories, paradigms and models, methods and techniques of inquiry available to a particular scientific school or worker[12]. This is the natural sequence of things, before any content is included in the field of science, it reveals itself in social spaces and constitutes the basis for formulated generalizations. "In this way social products, antecedently established knowledges capable of functioning as the transitive objects of new knowledges, are used to explore the unknown (but knowable) intransitive structure of the world"[13]. Knowledge in the transitive dimension differs from knowledge embedded in the intransitive dimension.

Defining intransitive objects of knowledge, Bhaskar states that "the intransitive objects of knowledge are in general invariant to our knowledge of them: they are the real things and structures, mechanisms and processes, events and possibilities of the world; and for the most part they are quite independent of us. They are not unknowable, because as a matter of fact quite a bit is known about them[14]. This citation is crucial in the epistemic realm. First, the language used to describe intransitive objects of knowledge is relatively stable; these are truths ultimately expressed within the framework of a given paradigm (as in the case of quantum physics and discoveries nominated for the Nobel Prize — knowledge that extends and deepens classical physics). Second, these truths are formulated in terms of causal laws. The intransitive dimension of science enables a coherent understanding of reality. The law of gravity, for example, belongs to the domain of intransitive knowledge — and knowing it, along with the observable fact that falling objects accelerate, no reasonable person would jump from the tenth floor.

---

[11]R. Bhaskar, *A Realist Theory of Science*, op. Cit., p. 52.
[12]R. Bhaskar, *Realistyczna teoria nauki*, trans. Katarzyna Zahorodna, [in:] M. Sikora (red.), *Realizm wobec wyzwań antyrealizmu. Multidyscyplinarny przegląd stanowisk*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011, p. 237.
[13]Ibidem, p. 239.
[14]R. Bhaskar, *A Realist Theory of Science*, op. Cit., p. 12.

Formulated in terms of true knowledge or scientific laws, the findings pertain to the operation of generative mechanisms. As Bhaskar states: "The goal of science, however, is to generate knowledge of the mechanisms of creating phenomena in nature that come together to generate a real and continuous variation of world phenomena"[15]. These mechanisms, disclosed through in-depth reflection, function independently of human activity. The assumption of the existence of beings independent of human perception constitutes a transcendental condition necessary for the advancement of scientific inquiry. In the context of critical realism, causal laws remain operative even in the absence of observable events, as they possess an intransitive character. "By saying that the objects of discovery and scientific research are 'intransitive' I mean the indication that they exist independently of any human activity; and by saying that they are 'structured' I mean that they are separate from the patterns of events that occur"[16].

The goal of epistemology is to understand how the world works—specifically, to identify the underlying forces, processes, or mechanisms that generate observable effects or events within the empirical domain. Within its foundational assumptions, critical realism draws a clear distinction between ontology and epistemology, yet acknowledges their analytical interdependence and mutual co-constitution[17]. Epistemic complexity allows for the formulation of knowledge that is not necessarily tied to direct ontological experience. Both ontological and epistemological assumptions are essential for defining social reality and making scientific knowledge possible.

The emergence of generative mechanisms and their causal powers occurs through the application of retroductive reasoning combined with abductive inference. Bhaskar defines these processes as follows:

“Abduction involves redescription or recontextualization, most usually (in CR research) in terms of a characteristic causal mechanism or process which serves to explain it. Retroduction involves imagining a model of a mechanism, which, if it were real,

[15]R. Bhaskar, *Realistyczna teoria nauki*, op. Cit., p. 231.
[16]R. Bhaskar, *A Realist Theory of Science*, op. Cit., 249.
[17] A. K. Albert, J. S. Brundage, P. Sweet i F. Vandenberghe, *Towards a critical realist epistemology?*, „Journal for the Theory of Social Behaviour” 50(3)/2020, p. 358, DOI: 10.1111/jtsb.12248.

would account for the phenomenon in question. (These two can often shade into each other: there is only a relative difference between them)”[18].

Abductive inference involves a reconfiguration of premises that leads to plausible conclusions, based on existing knowledge about the phenomenon under investigation. It offers an alternative to the limitations of purely inductive or deductive reasoning by proposing a logically grounded approach to problem-solving.

In contrast, the retroductive logic of model discovery entails imagining the necessary conditions for the existence of particular elements or phenomena. As Bhaskar describes it: "A thought operation involving a reconstruction of the basic conditions for anything to be what it is, or, to put it differently, it is by reasoning we can obtain knowledge of what properties are required for a phenomenon to exist." The transfactual or transcendental argument represents a form of retroduction, through which one seeks these essential properties beyond what is immediately given”[19].

Ethical assumption

The metatheory of critical realism provides a framework for addressing ethical questions from the standpoint of moral realism. Bhaskar articulates this position in the phase of Dialectical Critical Realism, where the pursuit of alethic truth, freedom, and justice is treated as intrinsically valuable. „Bhaskar’s argument for the universality of morality is a component of his dialectical critical realist ethics; this is a moral realist and ethical naturalist position that seeks to ground moral theory in an understanding of reality”[20]. This ontologically transcendental ethical dimension persists regardless of whether individuals explicitly recognize moral values in their everyday agency. The existence of social reality-itself ontologically real and constitutive of human subjectivity-renders moral agency immanently embedded in human action. Morality thus permeates real structures and activates moral powers capable of transforming the social world. It

[18]R. Bhaskar, *Foreword*, [In:] P. K. Edwards, J. O’Mahoney i S. Vincent (red.), *Studying Organizations Using Critical Realism. A Practical Guide*, Oxford University Press, Oxford 2014, p. VII.
[19]D. Berth, M. Ekstrom, L. Jakobsen, J. Ch. Karlsson, *Explaining Society: An Introduction to Critical Realism in the Social Sciences*, Pub. Routledge, London and New York 2001, p. 206.
[20]S. Ash, *Explaining Morality: Critical Realism and Moral Questions*, Pub. Routledge, London and New York 2022, p. 30.

constitutes the basis of the onto-axiological agency of every subject[21]. Morality constitutes the foundation of the onto-axiological agency of every subject.

Morality is embedded in the intransitive dimension of knowledge. As Steve Ash observes: "This can be understood as stating that moralities are transitive, but they have an intransitive object – intrinsic value[22]. In this view, the dogma of Weberian axiological neutrality is challenged. Values may resonate within subjective human agency, functioning not merely as normative declarations of what ought to be done, but as a transformative force shaping human action.

Critical and realistic data analysis in the area of Big Data

The Big Data environment is a collective term referring to large volumes of data, along with the capabilities for their storage, processing, visualization, and the development of conclusions based on them. There exists a strong relational interdependence among the components of the Big Data environment. In the relevant literature, it is often described as a socio-technological phenomenon, encompassing both social contexts-such as communities, collectives, and groups-and technological infrastructures[23]. Technologies associated with Big Data support a data-driven approach, which involves continuous responsiveness to real-time data outputs and the adaptation of practical actions accordingly[24]. The resulting high-velocity data streams, commonly referred to as Big Data, provide valuable material for research, whether for scientific, business, or other purposes.

When conducting research in the Big Data environment, it is important to recognize the numerous advantages offered by a critical realist approach. At the ontological level, data is embedded within a relatively broad social context and exhibits a high degree of complexity. Before contextualizing such data, it is essential to properly identify its ontological status. Understanding data begins with disclosing its sources of

[21]J. Mariański (red.), *Leksykon socjologii moralności. Podstawy – teorie – badania – perspektywy*, Zakład Wydawniczy NOMOS, Kraków 2015, p. 975.
[22]S. Ash, *Explaining Morality: Critical, op. Cit.* p. 42.
[23]D. Boyd, K. Crawford, *Critical questions for big data*, „Information, Communication & Society" 15(5)/2012, p. 663, DOI: 10.1080/1369118X.2012.678878.
[24]D. Stephenson, *Big data, nauka o danych i AI bez tajemnic. Podejmuj lepsze decyzje i rozwijaj swój biznes!*, transl. Wojciech Bombik, Pub. Helion, Gliwice 2020, p. 72.

origin and the properties ascribed to it. The emergent entities are initially expressed in natural language[25]. This requires a deeper reflection on their identity across the three layers of reality. One should proceed from the level of data (Domain of the Empirical), through the Domain of the Actual, and culminate in identifying the causal mechanisms within the Domain of the Real that generate observable regularities. This process involves the emergence of ontological entities and their intelligibility as epistemologically accessible phenomena[26].

The epistemic dimension, subordinate only to the ontic dimension, is essential in light of the scientific progress already achieved within the relevant field. When engaging in the pursuit of new knowledge, it is necessary to critically assess existing contributions. A thorough analysis of prior scientific achievements helps delineate the intransitive dimension of knowledge, which serves as the foundation for producing, modifying, or refining further knowledge. The researcher must possess a comprehensive understanding of the subject matter within their domain of inquiry. Attention should also be paid to international scholarship. In the era of globalization, access to knowledge across disciplines is merely a few clicks away.

An illustrative example is the issue of fear, which has become a frequent subject of inquiry among Big Data researchers, particularly through techniques such as sentiment analysis. From an ontological perspective, any form of existential uncertainty contributes to the dynamics of social change. Such change may occur in positive, negative or neutral forms.

Elemer Hankiss argues that existential security, which includes the fear of threats among other factors, has been a major driving force behind civilizational transformations. On the one hand, fear has influenced the structural dimension of society by becoming embedded in institutions responsible for ensuring broadly understood security. On the other hand, it has shaped the symbolic and protective sphere, including myths and religions, systems of values and beliefs, ideas and scientific theories, moral and practical

[25]V. Lytvyn, V. Vysotska, O. Veres, *Ontology of Big Data Analytics*, „MEST Journal" 6(1)/2018, p. 54, DOI: 10.12709/mest.06.06.01.06.
[26]Anonymous PWN, Warszawa 2021, p. 100 and next.

norms of behaviour, as well as a wide array of everyday rituals and trivialities[27]. Fear is undoubtedly an emotion that resonates with human action, either motivating individuals to act or causing them to withdraw. These responses can be broadly categorized into three general lines of action, although in practice more variations may exist. The first includes positive actions aimed at overcoming fear. The second involves inaction or the delegation of responsibility for creating safe living conditions to designated institutions. The third encompasses neutral responses, reflecting a reluctance or refusal to engage in any form of action.

An interesting feature of Big Data analysis is the involvement of experts from various scientific disciplines and professional backgrounds in the execution of such projects. Members of these interdisciplinary teams must develop a shared vocabulary that ensures mutual understanding. Another important aspect is that data on the observed phenomenon is collected in its entirety, which makes it possible to systematically monitor the phenomenon and identify recurring patterns.

„The data are not subject to every ontological framing possible, or every form of data-mining technique in the hope that they reveal some hidden truth. Rather, theoretically informed decisions are made as to how best to tackle a data set such that it will reveal information which will be of potential interest and is worthy of further research"[28].

When searching for generative mechanisms, it is necessary to define their components and the strength of the interactions between them. This allows for the identification of patterns or trends emerging from the data. It is important to take into account multiple competing causal forces and powers, and to select the most plausible ones through the application of retrodictive reasoning.

Critical realism established ontic and epistemic assumptions, which were later supplemented by axiomatic assumptions and those pertaining to the transcendental and even theological dimensions of reality. One of the main challenges in conducting research within the digital sphere is the maintenance of ethical standards, particularly those

[27]E. Hankiss, *Fears and Symbols: An Introduction to the Study of Western Civilization*, Pub. CEU Press, Budapest 2001, p. 1-2.
[28] R. Kitchin, *Big Data, new epistemologies*, op. Cit., p. 6.

already established in studies of the experienced, material world. Among the ethical concerns are issues related to data anonymization, methods of data collection, and the tracking of individuals without their informed consent. Determining the potential and actual impact of an algorithm in ethical terms is complex for several reasons. Assessing the influence of human subjectivity in the design and configuration of algorithms often requires the analysis of long-term, multi-user development processes[29].

Final conclusions

Researchers engaged in large-scale data analytics can successfully embed their analytical projects within the framework of critical realism. This perspective addresses the limitations of positivist and post-positivist paradigms, offering a more robust ontological and epistemological foundation for inquiry. Critical realism is increasingly recognized as a valuable approach to understanding social reality, including its digital dimensions[30]. Critical realists focus on mapping the ontological character of social reality, incorporating not only its structural and relational aspects but also its epistemological and axiological dimensions, particularly as they manifest in virtual contexts. The core assumptions of critical realism can thus be effectively applied to research on virtual reality, regardless of the specific subject of investigation. As a research programme, critical realism continues to provide a powerful framework for in-depth exploration of social reality. Reflecting on its theoretical foundations helps to overcome the epistemological and methodological limitations of earlier scientific approaches. It is also worth mentioning the interesting position of Krzysztof Wielecki:

"Virtual space is becoming a new type of social practice in which social, economic, political, cultural, and personal relations are produced, transformed, reproduced, or mediated, along with people's mentalities, values, imaginaries, and belief systems. In this way, life unfolds within a certain split between two dramatically emerging and competing realities at the turn of historical epochs: the virtual reality-largely dominated by mass culture, which appears more alluring, attractive, significant, interesting, and seemingly more true and real-and the other reality, which, by contrast,

[29]Mittelstadt B. D. et all., *The ethics of algorithms, op cit*., p. 2.
[30]K. Wielecki, *Prawda socjologiczna i realizm krytyczny*, „Rocznik Filozoficzny Ignatianum", XXIV(1)/2018, p. 67.

lacks these aforementioned qualities, but is also free from the shortcomings of the former”[31].

Virtual space has become a dominant arena of activity for many individuals. When studying virtual reality, it is essential to consider the specific conditions under which users engage with it. Researchers working within the framework of critical realism possess the conceptual tools necessary to analyse virtual phenomena, including those related to Big Data. Such sources can disclose new dimensions of knowledge that are mediated through transhumanist processes. Therefore, virtual spaces and the reality of the social world should be examined through a hybrid analytical lens, one that integrates both digital and social ontologies.

In conclusion, several key concepts developed throughout the article are crucial for understanding how critical realism can be applied to Big Data research. First, the stratified ontology (empirical–actual–real) provides a robust framework for distinguishing between observable data, the events they represent, and the underlying generative mechanisms. This stratification helps prevent empirical reductionism and supports deeper explanatory models.

Second, the distinction between transitive and intransitive dimensions of knowledge clarifies how scientific understanding is both socially produced and aimed at uncovering reality that exists independently of our cognition. In Big Data environments, this duality invites reflection on how algorithmic knowledge is constructed and how it can obscure or reveal deeper causal patterns.

Third, moral realism and ethical agency remind us that data analytics is not value-neutral. Ethical considerations-such as the anonymization of data, informed consent, and algorithmic accountability-are grounded in ontologically real moral structures that shape, and are shaped by, human action.

---

[31]K. Wielecki, *Kultura versus ~~Kultura~~ masowa. Podmiotowość i quasi-kultura w nibyspołeczeństwie*, Pub. Narodowe Centrum Kultury, Warszawa 2024, p. 595. Original text: Wirtualna przestrzeń staje się nowym rodzajem praktyki, w której wytwarzane, transformowane, reprodukowane lub zapośredniczane są stosunki społeczne, gospodarcze, polityczne, kulturowe, osobiste wraz z mentalnością, wartościami, wyobrażeniami, wierzeniami ludzi. W ten sposób życie przebiega w jakimś rozdwojeniu pomiędzy dwiema dramatycznie wyłaniającymi się i konkurującymi na przełomie epok rzeczywistościami: wirtualną – w ogromnej mierze zdominowaną przez kulturę masową, która wydaje się bardziej powabna, atrakcyjna, ważniejsza, ciekawsza, prawdziwsza i realna, i tą drugą, która – przeciwnie – nie posiada tych wcześniej wymienionych zalet, ale też brak jej wad tamtej.

Finally, the logic of discovery in Big Data should rely not only on induction or correlation but also on abduction and retroduction. These inferential modes allow researchers to formulate hypotheses about hidden mechanisms and necessary conditions for observed data patterns, moving beyond surface-level trends toward deeper causal explanations.

Together, these concepts form a critical-realist foundation for navigating the epistemic and ethical challenges of data-intensive research in the digital age.

References

AlbertA. K., Brundage J. S., Sweet P., Vandenberghe F., *Towards a critical realist epistemology?*, „Journal for the Theory of Social Behaviour" 50(3)/2020, p. 358, DOI: 10.1111/jtsb.12248.

Archer M. S., Collier A. Porpora D.V., *Transcendencja. Realizm krytyczny i Bóg*, transl. and Introduction: Artur Wysocki, epilog Krzysztof Wielecki, Pub. UKSW, Warszawa 2021.

Ash S., *Explaining Morality: Critical Realism and Moral Questions*, Pub. Routledge, London and New York 2022.

Berth D., Ekstrom M., Jakobsen L., Karlsson J. Ch., *Explaining Society: An Introduction to Critical Realism in the Social Sciences*, Pub. Routledge, London and New York 2001.

Bhaskar R., *A Realist Theory of Science*, with an Introduction by Mervyn Hartwig, Pub. Routledge, London and New York 2008.

BhaskarR., *Realistyczna teoria nauki*, trans. Katarzyna Zahorodna, [in:] M. Sikora (red.), *Realizm wobec wyzwań antyrealizmu. Multidyscyplinarny przegląd stanowisk*, Oficyna Wydawnicza Politechniki Wrocławskiej, Wrocław 2011.

BhaskarR. *Foreword*, [in:] P. K. Edwards, J. O'Mahoney i S. Vincent (red.), *Studying Organizations Using Critical Realism. A Practical Guide*, Oxford University Press, Oxford 2014, p. VII.

Bhaskar R., *Enlightened Common Sense: The Philosophy of Critical Realism*, In Introduction Mervyn Hartwig, Pub. Routledge, Abingdon 2016.

Biłobran Cz., *Społeczne konstruowanie operatorów dominacji nad zagrożeniami występującymi lokalnie na przykładzie powiatu nyskiego* https://repozytorium.uni.wroc.pl/dlibra/publication/144569/edition/133980/spoleczne-konstruowanie-operatorow-dominacji-nad-zagrozeniami-wystepujacymi-lokalnie-na-przykladzie-powiatu-nyskiego-bilobran-czeslaw

Boyd, Crawford K., *Critical questions for big data*, „Information, Communication & Society" 15(5)/2012, p. 663, DOI: 10.1080/1369118X.2012.678878.

Hankiss E., *Fears and Symbols: An Introduction to the Study of Western Civilization*, Pub. CEU Press, Budapest 2001.

Kitchin R., *Big Data, new epistemologies and paradigm shifts*, „Big Data & Society" 1(1)/2014, p. 3-6, DOI: 10.1177/2053951714528481.

Krzysztofek K., *Big Data Society. Technologie samozapisu i samopokazu*, „Transformacje. Pismo interdyscyplinarne", 1–4(72–55)/2012, pp. 223–257.

Anderson Ch., *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, https://www.wired.com/2008/06/pb-theory/ accesed 31 october 2024.

Lytvyn V., Vysotska V., Veres O., *Ontology of Big Data Analytics*, „MEST Journal" 6(1)/2018, p. 54, DOI: 10.12709/mest.06.06.01.06.

Mariański J. (red.), *Leksykon socjologii moralności. Podstawy – teorie – badania – perspektywy*, Zakład Wydawniczy NOMOS, Kraków 2015, p. 975.

Mingers J., Mutch A., Willcocks L., *Critical Realism in Information Systems Research*, „IS Quarterly" 37(3)/2013, p. 797, http://irep.ntu.ac.uk/id/eprint/20232/1/216160_300.pdf (accesed: 2 X 2024).

Mittelstadt B. D., Allo P. , Taddeo M., Wachter S. , Floridi L., *The ethics of algorithms: Mapping the debate*, „Big Data & Society" 3(2) (2016), p. 2, DOI: 10.1177/2053951716679679.

Porpora D.V, *A reflection on critical realism and ethics*, „Journal of Critical Realism" 18(3)/2019, p. 274, DOI: 10.1080/14767430.2019.1618064.

Savage M., Burrows R., *The coming crisis of empirical sociology*, „Sociology" 41(5)/2007, pp. 885–899, DOI: 10.1177/0038038507080443.

Stephenson D., *Big data, nauka o danych i AI bez tajemnic. Podejmuj lepsze decyzje i rozwijaj swój biznes!*, transl. Wojciech Bombik, Pub. Helion, Gliwice 2020.

Stochmal M., Relacyjna moc darów troski i ofiarność druhów Ochotniczych Straży Pożarnych: Perspektywa krytycznego realizmu i ontologii społecznej, Pub. PWN, Warszawa 2021.

Stochmal M., Krytyczny realizm Roya Bhaskara – Basic Critical Realism, „Uniwersyteckie Czasopismo Socjologiczne" 31(1)/2023, p. 12, DOI: 10.21697/ucs.2023.31.1.02.

Wielecki K., *Prawda socjologiczna i realizm krytyczny*, „Rocznik Filozoficzny Ignatianum", XXIV(1)/2018, pp. 45–70.

Wielecki K., *Kultura versus ~~Kultura~~ masowa. Podmiotowość i quasi-kultura w nibyspołeczeństwie*, Pub. Narodowe Centrum Kultury, Warszawa 2024.

Żulicki R, *Potencjał Big Data w badaniach społecznych*, „Studia Socjologiczne" 3(266)/2017, pp. 175–207.

„dot.pl" - czasopismo Rejestru domeny .pl

Latvia's Drone Diplomacy

Aleksandra Kuczyńska-Zonik
John Paul II Catholic University of Lublin: Lublin, Poland
ORCID: https://orcid.org/0000-0002-5672-9613
E-mail: kuczynska.a@gmail.com

Received: 04.09.2025
Accepted: 14.10.2025
Published: 14.10.2025

Cite this article as:
A. Kuczyńska-Zonik, "Latvia's Drone Diplomacy"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/212561

Corresponding author:
Aleksandra Kuczyńska-Zonik, Un John Paul II Catholic University of Lublin: Lublin, Poland

E-mail: kuczynska.a@gmail.com

Abstract

In 2024, Latvia and the United Kingdom initiated an international programme with the objective of providing Ukraine with unmanned systems, which was designated the Drone Coalition. The purpose of this initiative is to facilitate the delivering of drones to Ukraine, as well as the training of personnel in the utilisation of state-of-the-art technologies. From Latvia's standpoint, the project presents an opportunity to bolster its defence capabilities, foster domestic enterprises through research, and enhance its international reputation as an innovative nation. This initiative also represents a novel domain within the broader field of diplomacy, namely *defence innovation and production diplomacy* (DIPD).

Keywords: Latvia, Drones, Diplomacy, Technologies, Digitalization

Introduction

Since the beginning of the 21st century, Latvia has experienced dynamic economic development. However, the emergence of numerous challenges, including an ageing society due to population decline and emigration, the consequences of the 2008-2010 economic crisis (the global economic crisis affected Latvia much more severely than neighbouring countries), the pandemic of 2020, significant income disparities, and differences in regional development levels have forced the state to implement technological transformation and digitalization in its domestic policy[1]. Concurrently, contemporary technologies have had the potential to exert a substantial influence on Latvia's foreign policy. In recent years, in the face of Russia's aggression in Ukraine, Latvian diplomacy has sought to enhance its defence capabilities, foster domestic enterprises through the promotion of scientific research, and project an image of innovation on the global stage. Latvia's perspective on the role of modern technologies encompasses several key areas. Firstly, in the field of domestic policy, it is believed that modern technologies facilitate innovation and enhanced productivity within corporate entities as well as these technologies are recognised as a means of providing residents with access to public services, thereby contributing to the reduction of regional disparities[2]. It is in the line of the concept of resilience which concerns the ability of state or organisations to move quickly and seamlessly to adopt new technology solutions and then to recover, rebound, and move forward if things go wrong. Latvia's authorities emphasize technology development as a path of its transformation toward sustainability and prosperity. This also reflects the need for redesigning its institutional framework to enhance innovative and democratic systems. It should be underlined that Latvia, together with Estonia and Lithuania, appears in the top of IMD World Digital Competitiveness ranking evaluating the landscape of developing digital technologies and examining the level of preparedness of an economy to challenges in the future. Three Baltic states are among the most innovative countries in the Central European region, and their standings

[1] A. Kuczyńska-Zonik, *The Baltic States: Digital Democracy in the Era of the Pandemic*, IEŚ Policy Papers, no. 6, 2021.
[2] N. Wendt-Lucas, S. Jessen, M. Brynteson, *National Digital Inclusion Initiatives in the Nordic and Baltic Countries*, Nordregio Report, no. 3, 2024.

are gradually rising. This reflects the openness of the states to new, non-standard ideas. Additionally, those data show how economies employ new technologies, which could help react to serious challenges.

Secondly, in the area of foreign policy, the impact of modern technologies is considered significant in determining military development[3]. For smaller economies such as Latvian, investing in modern technology allows them to create niches and specializations, amplifying their impact despite limited resources. Finally, they can play a supportive role in enhancing and fostering cooperation between states, thereby influencing regional security.

This paper offers empirical evidence of utilization of modern technologies for diplomatic purposes by Latvia. Unmanned aerial vehicles (UAVs) known as drones are an example of advanced technology armament that offers a wide range of advantages across military, economic and diplomatic spheres. Drones are becoming a top priority for national defence sectors, promoting their wider integration into defence strategies. They encompass a broad spectrum of unmanned systems, including air, land, and maritime drones, as well as counter-drone solutions. Drones are inexpensive means for intelligence gathering and they can neutralize enemy defences, helping countries project power. They are easy to transport, enable high attrition rates with deniability, and can quickly strengthen local proxies. So far drones have been used for military power in conflicts in various regions, including Libya, Syria, Nagorno-Karabakh, and Ukraine. Drones may also become a core component of a country's foreign policy, helping it strengthen partnerships as seen between Turkey and Ukraine[4]. In the special geopolitical context of Russia-Ukraine war, an intention of this paper is to utilize a concept of drone diplomacy to define Latvia's foreign policy strategy and its drone technology as an integral asset to achieve military, economic and diplomatic objectives. Firstly, an aim is to present theoretical framework relating to technology, military and diplomacy. Then, the concept is tested using empirical date on Latvia's co-led initiative of drone

[3] See: M. Górka, *Cyber deterrence policies of the Baltic states in the years 2016–2023*, Rocznik Instytutu Europy Środkowo-Wschodniej, vol. 22, no. 1, 2024, pp. 45-66, DOI: https://doi.org/10.36874/RIESW.2024.1.3.

[4] F. Borsari, *Turkey's drone diplomacy: Lessons for Europe*, European Council on Foreign Relations, Commentary 31 January 2022.

cooperation in order to identify how new technologies in military domain may contribute to Latvia's diplomatic, military and economic potential and visuality.

Theoretical Framework

The concept of *defence* or *military diplomacy* encompasses the classic umbrella term for the activities of state institutions, especially defence ministries and armed forces through negotiations or other measures of a peaceful nature. It refers to the utilisation of diplomatic instruments and methodologies including engagement with other nations and international organisations to attain foreign policy objectives such as security, integrity and sovereignty[5]. It includes sets of practices such as: exchange of personnel, ships and aircraft, high-level visits and senior commanders, bilateral meetings and dialogue, training and exercises, regional defence forums, military assistance, confidence-building measures and non-proliferation, with an aim to build and maintain trust and help in the development of democratic armed forces[6].

In turn, the concept of *tech diplomacy* defines the relations of states with the technology sector and the governance of new technologies. This term confirms how the internet, advanced technologies, and social media platforms have become indispensable for diplomacy[7]. It is also important to emphasise that dual-use technologies represent a significant domain of policy and cooperation between states, frequently associated with security and defence. Nevertheless, a consensus on a single definition remains elusive. In order to denote the combination of defence and technology in the context of diplomacy the term *defence-tech diplomacy* is employed unofficially to link cutting edge technology expertise, high-tech business strategies, and foreign policy tools, to prevent authoritarian nations from using new technologies to expand their power and undermine precious freedoms[8]. It is the deliberate combination of defence diplomacy and technology diplomacy tools to shape access, development, transfer, and regulation of advanced

[5] https://www.diplomacy.edu/topics/defence-diplomacy/.
[6] A. Cottey, A. Forster, *Reshaping Defence Diplomacy: New Roles for Military Cooperation and Assistance*, Routledge 2004, p. 7; L. Drab, *Defence diplomacy – an important tool for the implementation of foreign policy and security of the state*, Security and Defence Quarterly, vol. 20, no. 3, 2018, pp. 57-71. doi:10.5604/01.3001.0012.5152.
[7] C. Bjola, M. *Kornprobst, Studying Tech Diplomacy—Introduction to the Special Issue on Tech Diplomacy*, Global Policy, vol. 1, no. 8, 2025. https://doi.org/10.1111/1758-5899.70035.
[8] https://techdiplomacy.org/tech-diplomacy/.

technologies (especially dual-use) for military capabilities, interoperability, and supply chain resilience. The strategy integrates conventional peacetime military instruments, such as visits, attachés, training, and agreements, with initiatives directed towards the technology sector, standards, and export controls. However, it should be noted that this term is more of a descriptive nature and does not constitute a technically recognised academic term.

Moreover, the advent of neologisms in this field, such as *production diplomacy*, underscores the coordination of supply chains and defence industries among allies, a concept that has been incorporated into the defence industry strategies of numerous nations. This phenomenon has calls for integrating the defence industrial bases of allies and partners and "provides opportunities to protect supply chains, strengthen alliances and partnerships, enhance deterrence, and build defence readiness" and is in relation to the US National Defence Industrial Strategy (NDIS), published in September 2023[9]. It emphasizes necessity to supplement the state investments as well as to maintain closer co-operation on defence industrial challenges with allies and partners as a top priority. *Defence production diplomacy* is similar term, defined as the coordinated diplomatic and industrial actions with allies and partners that integrate and scale arms production chains (co-development, co-production, co-sustainment) to increase capabilities, supply resilience, and interoperability. This is achieved through friend-shoring and joint investments in production capacity, and can be characterized by so-called "production-oriented diplomacy," a term that was discussed and popularised by in the NDIS[10]. Both p*roduction diplomacy* and *defence production diplomacy* should be seen as a strategy to protect supply chains, but it can support far more national security objectives, especially in the unpredictable geostrategic environment.

None of the aforementioned concepts have hitherto incorporated both innovation and advanced technology, as well as defence and diplomacy. Thus, it is suggested to introduce a concept of *defence innovation and production diplomacy* (DIPD) with an

[9] A. Brown, J.T. Watts, M. Garlauskas, *Production diplomacy for deterrence, readiness, and resilience in the Indo-Pacific*, Atlantic Council, June 27, 2024.
[10] National Defense Industrial Strategy, Department of Defense 2023, https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf

objective to define a coordinated diplomatic approach with allies and partners that fuses defence innovation (R&D, dual-use, deep tech) with scaled co-development, co-production and co-sustainment. While it focuses on accelerating capability deployment, strengthening supply chain resilience, and enhancing interoperability, DIPD consciously expands the already established *production diplomacy* with a distinct innovation module. It also combines defence innovation (R&D, dual-use, deep tech) with large-scale co-production (co-dev/co-prod/co-sustain). The following section provides empirical data on the DIPD concept based on Latvia's Drone Coalition.

Drone Coalition

Since Russia's full-scale invasion of Ukraine in February 2022, several European countries including Latvia have dynamized their activity for domestic military purposes and for the coordination of defence industrial support for Ukraine including defence equipment, training, and logistical support. The aim of these efforts has been to encourage and align international commitments to defence investment, production, and procurement actions. Particularly, UAVs play a critical role in the Ukrainian Air Force's efforts to resist Russian aggressor.

As a result, on 14 February, 2024, Latvia and the United Kingdom initiated an international project to provide Ukraine with unmanned aerial vehicles, so-called the Drone Coalition, in order to coordinate the Coalition's common fund and joint procurement to ensure the continuity of supplies of unmanned aerial vehicles to Ukraine. The commitment includes supplying Ukraine with combat drones of various capacities, developed in accordance with the requirements set by the Ukrainian armed forces. The Coalition currently includes 20 member states: Latvia, the United Kingdom, Australia, Belgium, the Czech Republic, Denmark, France, Estonia, Italy, New Zealand, Canada, Lithuania, Luxembourg, the Netherlands, Norway, Poland, Turkey, Ukraine, Germany and Sweden. The Drone Coalition's mission is threefold: firstly, to ensure the continued transfer of combat drones with various parameters, designed in accordance with the requirements of the Ukrainian Armed Forces; secondly, to develop the production of drone systems; and thirdly, to promote secure supply chains for these devices in Western countries.

In 2024, the total support provided to Ukraine by member states of the Drone Coalition amounted to €1.8 billion. At that time, Latvia allocated €20 million, and plans to allocate the same amount in 2025. An international fund with an endowment in excess of €80 million has also been operating within the Coalition since July 2024 (Latvia allocated €5 million for this purpose). In accordance with the contracts signed in January 2025, with a total value of €54 million, the Coalition is obligated to provide Ukraine with 30,000 drones. Two Latvian companies are also involved in the production process, and it is anticipated that they will deliver 12,000 drones with a total value of €17 million.

Latvia's involvement in the Drone Coalition has resulted in substantial advancements in the production of unmanned aerial vehicles, thereby stimulating industries that utilise contemporary technologies. This initiative has had the effect of strengthening the country's defence potential, whilst concomitantly creating new opportunities for local entrepreneurs, the research sector, and the defence industry. Participation in the Coalition furnished Latvia with access to the knowledge and experience gained during the war in Ukraine, funding for technology development, and the opportunity to test and develop cutting-edge drone solutions through international public procurement. These initiatives have enabled Latvia to develop concepts for new devices and to develop its own combat capabilities, while Latvian companies have gained the opportunity to participate in international tenders and to promote their brands on the global market. For instance, Latvia hosted the "Drones for Ukraine" hackathon and launched the Latvian Drone Capabilities Development Initiative to enhance the drone capabilities of the Latvian Armed Forces. In June 2024, a testing ground was also established at the Sēlia military training ground, where both domestic and foreign drone manufacturers can conduct tests on developing technologies using unmanned aerial vehicles. In October 2024, Origin, a Latvian company specialising in advanced autonomous systems, received €4 million in funding from the European Defence Fund for drone innovation.

Latvia’s leadership in drone diplomacy

The endeavours of Latvia's political authorities to furnish technological assistance to Ukraine have resulted in the advancement of the European and particularly Latvian drone industry. Latvia is consolidating its position in this field by maintaining its support for

Ukraine (in the previous year, it furnished Ukraine with almost 5,000 drones), advocating for the advancement of the domestic defence industry, fostering business collaboration, and catalysing innovation. In addition, Latvia's Competence Centre for Autonomous Systems was established to develop unmanned aerial vehicle technology and explore cutting-edge solutions to address the threats posed by drones to critical infrastructure. In general, Latvia has fostered domestic drone production, stimulated technological innovation, and deepened international partnerships.

Latvia's active role within the Drone Coalition presents an essence of *drone diplomacy*. The term covers the deliberate use of drones—and the policies governing their development, export/transfer, co-production, training, and regulation—as tools of statecraft: from signalling and power projection (ISR/strike) to deepening partnerships via sales, co-production and training, to soft-power humanitarian uses and the shaping of UAV norms. Latvia's strategic ambition in this regard is twofold: firstly, to develop and promote domestic drone technologies on a global scale, and secondly, to shape the image of an innovative country. Firstly, this format has fostered active exchange of information on research and innovation in the field of unmanned aerial vehicles, creating opportunities for countries to organise joint projects in the future. The Drone Coalition has been demonstrated to enhance Latvia's security, as the advancement of robotics and artificial intelligence has the potential to furnish optimal defence capabilities against asymmetric threats. It is also important for the development of the drone industry in Latvia, security of supply, and strengthening the national economy. Secondly, Latvia's effort to become European leader in the field of so-called *drone diplomacy* was demonstrated at the international Drone Summit in Riga, on 28 May, 2025, with the participation of the Latvian Ministry of National Defence and Riga University of Technology. Representatives of Drone Coalition member states, military experts, scientists, entrepreneurs, and leaders from the unmanned aerial vehicle industry attended the Summit, discussing the Coalition's achievements. The Summit also aimed to provide Latvian companies and researchers with opportunities to network with international partners and to encourage the optimal use of research potential in the defence industry. This event provided an additional platform for discussion and future

directions, with a particular focus on challenges related to global security and new dimensions of warfare.

Conclusions

Without any doubts the advent of modern technologies, including drones, has precipitated a fundamental shift in warfare tactics. In the context of Russia full-scale aggression, it is evident that drones have become a significant component of Ukraine's military apparatus, particularly in reconnaissance and strike missions. This analysis contributes to this fields with a special attention to drones and their role for military, economy and diplomatic purposes. Firstly, the focus was on theoretical consideration on innovative technology in defence sector and diplomacy. While some definitions were proposed to denote the current roles of advanced technologies for domestic and foreign policies, DIPD aligns allied defence innovation with scaled co-development/co-production to accelerate fielding, build supply-chain resilience, and improve interoperability. For example, Turkey's foreign policy strategy shows how a country utilizes its drone technology as an integral asset to achieve diplomatic, economic, and military objectives. Latvia has potential for innovation and defence technology development, too. It has a reliable technology infrastructure, effective digital policy and it ranks in good positions in terms of digital development in Europe, which results in Latvia being recognize as an innovative and digitally developed country. Autonomous military drones are stealthy and multi-domain integrated, and have been transforming modern warfare with AI. The "drone army" enhances national capabilities which is now one of its priority for Latvia's defence sector. By developing its own unmanned systems and counter-drone systems, Latvia builds its resilience and security. Additionally, drone diplomacy as an illustration of DIPD aims at strengthening alliances and partnerships, enhancing deterrence and building defence readiness. From Latvia's standpoint, the concept offers the prospect of enhancing its own defence capabilities, fostering the growth of domestic enterprises through the utilisation of scientific research, and projecting an image of an innovative nation on the global stage. Both the International Drone Summit and the Competence Centre for Autonomous Systems provide an opportunity to strengthen Latvia's leadership role in this regard. Latvia's co-leadership in

the Drone Coalition serves as an additional means of pressuring national, EU, and international structures to improve procedures, procurement issues, and investment efforts in the defence sector. It helps to collectively change the approach of EU and NATO members towards a "full-time-war logic" needed to support Ukraine.

In essence, for Latvia, drone diplomacy is not just about military hardware; it's a strategic pathway to enhance its international standing, stimulate economic growth through specialized defence production, foster technological innovation, and strengthen its national defence and alliances in a rapidly evolving geopolitical landscape. It allows Latvia to be a central node in a critical technological domain, much like a specialized gear within a larger, complex machine, contributing significantly to its overall function and direction.

References

Bjola C., Kornprobst M., *Studying Tech Diplomacy—Introduction to the Special Issue on Tech Diplomacy*, Global Policy, vol. 1, no. 8, 2025. **https://doi.org/10.1111/1758-5899.70035**

Borsari F., *Turkey's drone diplomacy: Lessons for Europe*, European Council on Foreign Relations, Commentary 31 January 2022

Brown A., Watts J.T., Garlauskas M., *Production diplomacy for deterrence, readiness, and resilience in the Indo-Pacific*, Atlantic Council, June 27, 2024

Cottey A., Forster A., *Reshaping Defence Diplomacy: New Roles for Military Cooperation and Assistance*, Routledge 2004

Drab L., *Defence diplomacy – an important tool for the implementation of foreign policy and security of the state*, Security and Defence Quarterly, vol. 20, no. 3, 2018, pp. 57-71. doi:10.5604/01.3001.0012.5152

Górka M., *Cyber deterrence policies of the Baltic states in the years 2016–2023*, Rocznik Instytutu Europy Środkowo-Wschodniej, vol. 22, no. 1, 2024, pp. 45-66, DOI: https://doi.org/10.36874/RIESW.2024.1.3

Kuczyńska-Zonik A., *The Baltic States: Digital Democracy in the Era of the Pandemic*, IEŚ Policy Papers, no. 6, 2021

National Defense Industrial Strategy, Department of Defense 2023, https://www.businessdefense.gov/docs/ndis/2023-NDIS.pdf

Wendt-Lucas N., Jessen S., Brynteson M., *National Digital Inclusion Initiatives in the Nordic and Baltic Countries*, Nordregio Report, no. 3, 2024

Web sites
https://www.diplomacy.edu/topics/defence-diplomacy/
https://techdiplomacy.org/tech-diplomacy/

„dot.pl" - czasopismo Rejestru domeny .pl

Sharp power w strukturze sieci polsko - białoruskiego konfliktu hybrydowego

„(...) cała struktura władzy spajająca do tej pory świat ulega dezintegracji. Równocześnie kształtuje się całkowicie nowa struktura władzy. I dokonuje się to na każdym szczeblu społeczeństwa".
A.Toffler, Zmiana władzy

Dawid Błaszczak
Akademia Bialska im. Jana Pawła II, Polska
ORCID: https://orcid.org/0000-0001-7335-8343
E-mail: dawid-blaszczak@wp.pl

Streszczenie

Niniejszy artykuł stanowi próbę socjologicznej analizy *„sharp power"* jako narzędzia po które skutecznie sięgają aktorzy współczesnych konfliktów hybrydowych. Prezentowany materiał teoretyczno-empiryczny w sposób dwutorowy uzupełnia lukę badawczą na gruncie zarówno nauk socjologicznych jak również nauk o bezpieczeństwie. Pierwszym krokiem jest próba usystematyzowania kategorii *„sharp power"*, na drodze „osadzenie jej" na kanwie socjologicznych teorii władzy. Drugim aktem jest sięgnięcie do analizy sieciowej, będącej nowatorską perspektywą badawczą odwzorowującą rozkład *„sharp power"* w strukturze sieci powiązań w ramach polsko-białoruskiego konfliktu hybrydowego.

Słowa kluczowe: konflikt hybrydowy, sieci społeczne, pogranicze polsko- białoruskie, *„sharp power"*

Received: 27.08.2025
Accepted: 06.11.2025
Published: 07.11.2025

Cite this article as:
D. Błaszczak, *"Sharp power w strukturze sieci polsko - białoruskiego konfliktu hybrydowego"*

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/214040

Corresponding author:
Dawid Błaszczak, Akademia Bialska im. Jana Pawła II, Polska
E-mail: dawid-blaszczak@wp.pl

Sharp power in the network structure of the Polish-Belarusian hybrid conflict

Abstract

This article attempts to sociologically analyze "sharp power" as a tool effectively utilized by actors in contemporary hybrid conflicts. The theoretical and empirical material presented addresses a research gap in oth sociological and security sciences in a two-pronged approach. The first step is to systematize the "sharp power" category by grounding it in sociological theories of power. The second step is to utilize network analysis, an innovative research perspective that maps the distribution of "sharp power" within the network structure of the Polish-Belarusian hybrid conflict.

Keywords: hybrid conflict, social networks, Polish-Belarusian border, "sharp power"

Wprowadzenie

Otaczająca nas rzeczywistość społeczna podlega permanentnym przeobrażeniom, wyrazem których jest obecność procesów i zjawisk o nowych cechach i uwarunkowaniach reorganizujących dotychczasowy układ geopolityczny, jak również transformujących proces władzy. Tradycyjnie rozumiana władza jako zdolność do wywierania wpływu przy pomocy militarnych środków określanych mianem twardych atrybutów władzy, uzupełniona zostaje o narzędzia manipulacji, dezinformacji oraz perswazji, w literaturze przedmiotu znane jako *„sharp power”*.

Celem niniejszego artykułu jest analiza *„sharp power”* jako narzędzia z powodzeniem stosowanego we współczesnych konfliktach hybrydowych, będących przykładem istotnego procesu zmian jakościowych na polu wojen kinetycznych i niekinetycznych. Prezentowane opracowanie stanowi wycinek interesującego obszaru eksploracji, odpowiedniego do aplikacji na grunt nauk socjologicznych i nauk o bezpieczeństwie, ze szczególnych uwzględnieniem socjologii pogranicza czy socjologii

bezpieczeństwa. Wartością dodaną niniejszego materiału jest próba usystematyzowania kategorii *„sharp power”* z położeniem nacisku na ewolucyjny charakter analizowanego procesu, którego forma, specyfika i zasięg ulegają permanentnym zmianom. Na potrzeby opracowania sięgnięto po wybrane metody i techniki badawcze, takie jak: analiza przypadków, analiza danych statystycznych i stanu literatury przedmiotu oraz analiza sieci społecznych, zakorzeniona w matematycznej teorii grafów.

Sieć – nowy paradygmat nakreślania natury i struktury świata

Metafora sieci coraz intensywniej oddziałuje na percepcję i objaśnianie otaczającej nas rzeczywistości społecznej, nakreślając przy tym paradygmat myślenia oraz konceptualizacji świata. Wiek XXI naznaczony jest symboliką sieci, będącej ideą i metamodelem świata, redefiniującym szeroko rozumiany proces spojrzenia na świat. „Dziś coraz częściej mówi się o sieciach (...) i nie jest to (...) zmiana terminologii, jest to raczej zmiana paradygmatu”[1]. Kierunek ten uwarunkowany jest następującymi czynnikami: po pierwsze, przybierającą na sile rewolucją technologiczną, która przy pomocy internetu i urządzeń mobilnych „pożera” wszystkie aspekty życia społecznego, powodując, że sieć... jest zawsze i wszędzie (*semper et ubique*). Po drugie, sieć jako natura, a zarazem struktura determinuje całe spektrum procesu transformacji dzisiejszej cywilizacji w tym informacji, obrazów i symboli generujących kierunek i natężenie zmian społecznych. Po trzecie, sieć, w dobie upowszechnienia internetu, jako warunku *sine qua non* dla urynkowienia oraz utowarowienia informacji, przybiera formułę dominującej przestrzeni przepływu informacji, opisujących bądź świadomie kreujących splot wydarzeń społecznych, politycznych, ekonomicznych. „Internet, jego rola i sposób funkcjonowania, stają się (...) metaforą dzisiejszej cywilizacji. Osią tej metafory jest pojęcie sieci”[2]. W podobnym akcencie wypowiada się Manuel Castells dla którego sieć „(...) to struktura społeczna utworzona wokół sieci komunikacji cyfrowej (...)”[3]. Autor uwypukla walory struktur sieciowych, takie jak elastyczność i zdolność do

[1] M. Muraszkiewicz, *Esej: nowy paradygmat, czyli od systemu do sieci*, [w:] B. Sosińska-Kalata i inni (red.), *Od informacji naukowej do technologii społeczeństwa komunikacyjnego*, Warszawa 2005, s. 83.
[2] Tamże, s. 84.
[3] M. Castells, *Władza komunikacji*, Warszawa 2013, s. 16.

samokonfiguracji, będące gwarantem skuteczności struktur. „W sieciach społecznych (...) aktorzy społeczni programują cele i procedury operacyjne”[4].

Patrząc przez pryzmat literatury przedmiotu, w tym opracowań encyklopedycznych oraz leksykalnych sieć to zbiór obiektów społecznych, zwanych węzłami lub aktorami oraz powiązań (połączeń) i przepływów między nimi[5]. Znaczenie części składowych sieci jest zróżnicowane i uwarunkowane programem sieci oraz stopniem i zakresem zdolności węzłów do maksymalizacji skuteczności struktury sieciowej na końcu której stoją wyznaczone cele mającego ścisłe odzwierciedlenie w „zainstalowanym” programie sieci. Z punktu widzenia świata, w tym gospodarki i geopolityki, opartej na informacji znaczenie przybiera na sile wraz z rosnącą efektywnością w zakresie gromadzenia, przetwarzania a także upowszechniania informacji. „Produktem” finalnym tak rozumianej logiki działań jest podbój umysłów oraz tworzenie ram znaczeniowych, kreujących ludzkie emocje, poznania i przekonania.

Przybierająca na sile i wydźwięku teza o społeczeństwie sieci stanowi dowód, że otaczające nas ekonomiczne, polityczne oraz społeczne zjawiska i procesy przyjmują formę sieciową, w której konfiguracja uwarunkowana jest charakterem połączeń, specyfiką zasobów czy pozycją, zajmowaną przez poszczególne węzły w sieci, a w końcu również programem samej sieci. W opinii Manuela Castellsa „społeczeństwo sieci (...) składa się z sieci obejmujących sfery produkcji, władzy i doświadczenia, tworząc kulturę wirtualną, kulturę przypływu globalnych trendów, przekształcających czas i przestrzeń”[6]. Sieć jako realny byt redefiniuje również klasycznie rozumianą kategorię władzy, bowiem jak zaznaczył Darin Barney „(...) władza i bezsilność są funkcją dostępu do sieci i kontroli przepływów”[7]. Te z kolei mogą przybierać różnorodną postać - zasobów materialnych i niematerialnych: ludzi, pieniędzy czy informacji, które o obecnym czasie kreują szeroko rozumianą politykę, kreśląc nowe ramy władzy, skoncentrowanej na gromadzeniu, przechowywaniu oraz dystrybucji informacji. „Nowe formy polityki są tym samym politykami walczącymi o zarządzanie informacjami i kontrolę w „przestrzeni” opanowanej

[4] Tamże, s. 33.
[5] Zob. M. Castells, *Władza...*, s. 33; D. Barney, *Społeczeństwo sieci*, Warszawa 2008, s. 37; T. Sozański, *Sieć społeczna*, [w:] *Encyklopedia Socjologii*, tom 4, Warszawa 2005, s. 28.
[6] M. Castells, *Koniec Tysiąclecia*, Warszawa 2009, s. 380.
[7] D. Barney, *Społeczeństwo...*, s. 41.

przez media (...) jako niezbędne warunki wstępne dla dostępu do bardziej materialnych form władzy”[8]. Na naszych oczach dokonuje się rekonstrukcja klasycznie rozumianej polityki, w tym potęgi sił (władzy), która opleciona została przez mniej lub bardziej gęstą sieć mediów, kreujących otaczającą rzeczywistość, wyzwalających określone zachowania i konstruujących nowy (nie) porządek świata. Trafnie zauważył Manuel Castells, że „(...) niezdolność (...) aktorów instytucji (...) do umiejętnego dostosowania się do „polityki z udziałem mediów informacyjnych” (...) jest „podstawowym źródłem kryzysu demokracji w Erze Informacji”[9].

Patrząc przez pryzmat narzędzia analitycznego i bytu realnego sieć jest zbiorem punktów (węzłów) połączonych ze sobą powiązaniami lub przepływami o określonej treści lub wartości. Przepływy zaś to nic innego jak strumienie informacji, przekazywane w obrębie sieci, definiujące cele oraz zasady działania tej sieci (program), promujące przy tym własne korzyści. „Sieci są więc skomplikowanymi strukturami komunikacyjnymi, powstałymi wokół zbioru celów (...). W sieciach (...) aktorzy (...) programują cele i procedury operacyjne”[10].

Sieć jako nowa agora władzy komunikacji i narzędzie wojny hybrydowej

Potrzeba studiów nad uchwyceniem współczesnej władzy w kategoriach sieciowych uzasadniona jest kilkoma przesłankami. Po pierwsze, mamy do czynienia z nasilającą się amalgamacją komunikacji i władzy. Fundamentem tego rodzaju amalgamacji jest możliwość kontroli ludzkiego umysłu, a w dalszej perspektywie sterowania zachowaniami i decyzjami społecznymi. „Władzę sprawuje się za pośrednictwem (...) struktur znaczeniowych (...) na podstawie dyskursów, które ukierunkowują działania aktorów społecznych”[11]. Po drugie, wkomponowanie władzy do kategorii sieciowej wynika z faktu, że władza przyjmuje postać relacji, jest – jak podkreślił M. Castells – zdolnością relacyjną, i nie można jej rozpatrywać w oderwaniu od aktorów społecznych. Po trzecie, próba identyfikacji socjoprzestrzennych sieci władzy jest skutecznym podejściem analitycznym w sytuacji gdy społeczeństwa

[8] Tamże, s. 144.
[9] M. Castells, *Władza...,* s. 312.
[10] Tamże, s 32.
[11] Tamże, s. 23.

„(...) składają się z licznych, (...) wzajemnie oddziałujących na siebie sieci władzy”[12]. Po czwarte, współczesne przestrzenie, które w opracowaniach wspomnianego już M. Castellsa definiuje się jako przestrzenie przepływów, przybierają formę technologicznie zasilanych sieci komunikacyjnych, zdolnych do generowania przepływów (np. informacji) niezbędnych do realizacji wspólnych zadań, osiągania celów, itp. Po piąte, wraz z upływem czasu, źródła władzy, w dalszym ciągu, zachowują swoją formułę, trwając w postaci dyskursu, przymusu i perswazji – wzmocnionych przez określone ramy kulturowe i optykę polityczną. Ewolucja dokonuje się zaś w obrębie terytorium, na którym rozlewają się ów relacje władzy. Klasycznie rozumiana przestrzeń fizyczna zostaje uzupełniona, docelowo zastąpiona – przez sieć. „W społeczeństwie sieci władza została zredefiniowana ale nie zanikła”[13]. Po szóste, patrząc na świat przez optykę wszechobecnej informacji, ikonograiki i wizerunku, specyficznych dla epoki cyfrowej, warto podkreślić, że współczesne mechanizmy polityki i dyplomacji, w tym również prowadzenia konfliktów, oparte są na sieciach komunikacyjnych, a konstruowanie władzy dokonuje się przez tworzenie obrazów. Trafnie zauważa M. Castells, że „(...) relacje władzy opierają się w dużej mierze na kształtowaniu ludzkich umysłów za pomocą tworzenia obrazów”[14].

Poruszając się w obrębie problematyki władzy w strukturze sieci nie sposób pominąć faktu, że kolejnym elementarnym zalążkiem potęgi jest zdolność sieci do zainicjowania a w dalszej kolejności kreowania określonych programów, które w nomenklaturze językowej M. Castellsa określano mianem „programów sieci”. W wymiarze praktycznym to możliwość tworzenia, dystrybuowania i moderowania informacją i dyskursem, które determinują ludzkie zachowania, sposób myślenia i działania. Formuła ta wpisuje się w aktualny (nie)porządek i logikę funkcjonowania świata, gdzie „(...) dyskursy kształtują myślenie za pośrednictwem określonych technologii (...) które organizują uspołecznioną komunikację”[15]. Skonstruowane w ten sposób pole semantyczne, w którym przekaz to jednocześnie medium powoduje, że tradycyjnie rozumiana polityka rozlewana jest w sieciach medialnych, będących areną kreowania władzy. Media ustanawiają przestrzeń,

[12] M. Mann, *The Sources of Social Power*, Cambridge 2000, s. 1.
[13] M. Castells, *Władza...*, s. 60.
[14] Tamże, s. 199.
[15] Tamże, s. 63.

w której kształtują się relacje władzy między współzawodniczącymi aktorami politycznymi i społecznymi. W związku z tym (...) wszyscy aktorzy i wszystkie komunikaty muszą „przejść" przez media, żeby móc osiągnąć swój cel"[16].

Punktem wyjścia do poniższego dyskursu będzie próba operacjonalizacji oraz delimitacji kluczowych kategorii teoretycznych, zogniskowanych wokół tłumaczeniowego i kontekstualnego znaczenia takich terminów jak struktura sieci czy władza (siła, potęga). Warto podkreślić, że obydwa pojęcia to niezwykle pojemne i szerokie spektrum znaczeniowe, obecne w socjologii, ale również w politologii, ekonomii czy naukach o bezpieczeństwie. Na łamach Encyklopedii Socjologii napisano, że „Władza jest fenomenem wieloaspektowym. (...). Jest stosunkiem społecznym i instytucją (...)"[17]. Wielostronny charakter władzy akcentowany jest również Piotr Sztompka, pisząc, że „(...) to zjawisko przenikające życie społeczne we wszystkich jego obszarach, obecne we wszystkich społeczeństwach (...)"[18]. Koncepcji tego typu wtóruje Michel Foucault podkreślając, że „władza jest podstawowym i uniwersalnym zjawiskiem społecznym"[19]. Pochylając się nad kategorią władzy nie sposób pominąć faktu, że „(...) należy je rozumieć nie jako mocarstwo, ale jako dany rodzaj siły tego mocarstwa lub dany rodzaj sposobu wywierania przezeń wpływu na pozostałe"[20]. Co więcej, na przełomie ostatnich kilkunastu lat, wskutek rekonfiguracji stosunków międzynarodowych, w tym rekompozycji układu sił, badania nad pomiarem władzy przyjęły wielowektorową ścieżkę, wyzwalając takie kategorie jak: *„smart power"*, *„linking power"* i *„sharp power"*[21]. Tym samym we współczesnym świecie dokonano rekonstrukcji układu sił, pozostawiając przy tym permanentne stanowisko o dążeniu do władzy jako fundamencie działania państw i struktur ponadpaństwowych. „Potęga państwa czy innych (...) grup społecznych jest najważniejszą właściwością ludzkiego działania, a jego logika pozostaje niezmienna w historii – zmieniają się tylko narzędzia (technologia) i warunki otoczenia (...)[22]. Należy przez to rozumieć zakorzenienie w logikę sieciową, w której władza „to coś, co płynie,

[16] Tamże, s. 200.
[17] W. Kubiak, *Władza*, [w:] *Encyklopedia socjologii*, tom 4, Warszawa 2005, s. 324.
[18] P. Sztompka, *Socjologia. Analiza społeczeństwa*, Kraków 2002, s. 69.
[19] J. Szacki, *Historia myśli socjologicznej*, Warszawa 2004, s. 907.
[20] M. Lisewski, *Soft power, sharp power, linking power. Mocarstwowe sposoby działania Chin i ich znaczenie dla świata*, Toruń 2021, s. 43.
[21] Por. M. Sułek, E. Szymala, *Potęga państw 2025. Ranking potęgometryczny*, Warszawa 2025, s. 5.
[22] M. Lisewski, *Soft...*, s. 8.

przemieszcza się, stając się coraz bardziej niezależne od określonego terytorium czy przestrzeni (...)”[23]. Pierwiastek sieciowy akcentuje Michel Foucault, zdaniem którego władzę „(...) sprawuje się w sieci, a po tej sieci jednostki nie tylko krążą, ale też zawsze znajdują się w pozycji, która każe im zarazem władzy podlegać i ją sprawować, (...)”[24]. Patrząc zatem przez okulary analityczne, w badaniach nad wieloaspektową władzą istotne znaczenie ma fakt „(...) by uchwycić władzę u jej granic, w jej najdalszych rozgałęzieniach, (...), w jej formach i instytucjach”[25].

Elementem tak rozumianego oddziaływania jest *„sharp power”* (ostra siła), która w węższym ujęciu jest „(...) perswazją manipulacyjną, z celowym przedstawianiem rzeczy nie takimi, jakie są, ale takimi, jakie mają być odbierane”[26]. Co więcej, „(...) wykorzystuje perswazję, a konkretnie manipulację (...) nie po to (...), aby uatrakcyjnić swój poziom, ale obniżyć atrakcyjność konkurenta”[27]. Zasobowe podejście do władzy postuluje Anthony Giddens, dla którego zasoby to nic innego jak różnego rodzaju środki, przy użyciu których sprawowana jest władza. Autor nakreśla znak równości pomiędzy władzą a zdolnością do osiągania założonych wyników działań. W analogicznym tonie wypowiadał się Talcott Parsons spoglądając na władzę przez pryzmat umiejętności działania czy wykonywania określonych funkcji społecznych. Z perspektywy czasu spojrzenie na władzę ulega redefinicji w kierunku perspektywy sieciowej. „Podejście sieciowe rzuca (...) nowe światło na problematykę władzy i wpływu. Przewagę nad innymi daje nie tylko posiadanie cennych zasobów, ale i szczególne umiejscowienie w sieci”[28]. Ugruntowani wielowymiarową oraz wieloaspektową logiką władzy „(...) jesteśmy świadkami kształtowania się kolejnego rodzaju oddziaływania reżimów politycznych na podmioty stosunków międzynarodowych, łączącego (...) elementy przymusu i manipulacji”[29]. Szeroką perspektywę analizy i deskrypcji władzy (potęgi) państwa prezentuje John G. Stoessinger, dla którego jest to nic innego jak „(...) zdolność państwa do użycia swoich

[23] J. Urry, *Socjologia mobilności*, Warszawa 2004, s. 171
[24] M. Foucault, *Nadzorować i karać*, Warszawa 2006, s. 516.
[25] Tamże, s. 516.
[26] M. Lisewski, *Soft...*, s. 74.
[27] Tamże, s. 75.
[28] T. Sozański, *Sieć społeczna* [w:] *Encyklopedia socjologii*, tom 4, Warszawa 2005, s. 29.
[29] Ł. Skoneczny, B. Cacko, *Sharp power – wprowadzenie do problematyki*, „Przegląd Bezpieczeństwa Wewnętrznego”, nr 13/2021, s. 102.

materiałów (...) w sposób, który wpłynie na zachowanie innych państw”[30]. W amerykańskiej opinii publicznej i przestrzeni dyskursu naukowego *„sharp power”* polega na penetrowaniu przestrzeni informacyjnej połączonej z praktykami manipulacyjnymi mającymi na celu dyskredytację określonego państwa lub środowiska społeczno-politycznego na oczach docelowej opinii publicznej. Jest to nic innego jak „(...) agresywne działania państwa prowadzone przy wykorzystaniu metod imitujących elementy soft power w celu manipulacji wizerunku danego kraju (...) bądź destabilizacji jego systemu społeczno-politycznego, bądź wymuszenia określonego postępowania jego władz”[31]. Niezależnie od rodzaju oraz potencjału zasobów elementarne znaczenie w budowaniu skutecznej polityki *„sharp power”* przypisać należy konieczności posiadania pogłębionej wiedzy na temat posiadanego wachlarza możliwości oddziaływania na innych aktorów, oplecionych siecią stosunków międzynarodowych. Analizując dostępną w przestrzeni społecznej dyskusję nad problematyką *„sharp power”* warto uwypuklić obecność sprzecznych ze sobą stanowisk – od uznania „ostrej władzy” za powszechny element budowania potęgi państw, po sprowadzenie jej do następstwa nieefektywnego łączenia miękkiej i twardej siły (*„soft power”, „hard power”* – przyp.).

Sharp power w teatrze działań wojennych/wojny hybrydowej - refleksje interdyscyplinarne

Interdyscyplinarny aspekt polemologii jako dyscypliny ukierunkowanej na badania konfliktów zbrojnych, pomimo swojej krótkiej historii ale długiej przeszłości, dostarcza bogatego spektrum wiedzy teoretycznej i metodologicznej na temat natury i morfologii wojny jako zjawiska społecznego. Patrząc przez pryzmat niniejszego artykułu kluczowe znaczenie przypisać należy studiom określającym wojnę: po pierwsze jako narzędzia polityki, po drugie w kategoriach konfliktu społecznego. Sięgając do optyki politologicznej podkreślić należy, że teatr działań wojennych jest instrumentem uprawiania polityki. „Wojna jest nie tylko czynem politycznym lecz (...) prawdziwym narzędziem politycznym, dalszym ciągiem stosunków politycznych, przeprowadzeniem ich innymi środkami”[32]. Spoglądając z kolei przez pryzmat socjologii zmagania wojenne to konflikty będące

[30] J. G. Stoessinger, *The Might of Nation. World Politics in Our Times*, New York, 1969, s. 26-27.
[31] Ł. Skoneczny, B. Cacko, *Sharp...*, s. 106.
[32] C. von Clausewitz, *O wojnie*, Lublin – Zamość 1995, s. 23.

nieuniknionymi zjawiskami, w których określony aktor społeczny (w tej roli: jednostka, grupa, państwo) próbuje osiągnąć własne cele w drodze podporządkowania, zniszczenia lub zniewolenia innego aktora społecznego. „Wyrasta on na gruncie nagromadzonych sprzecznych emocji, a objawia (...) wybuchem wrogich (...) postaw”[33].

Aktualnie prowadzony dyskurs nad przyczynami, dynamiką i skutkami wojen zostaje wzbogacony o nowy zakres semantyczny, przejawiający się w mnogości mniej lub bardziej nieostrych pojęć, takich jak: wojna nieregularna, wojna informacyjna, wojna sieciowa, wojna hybrydowa, wojna psychologiczna, cyberwojna, itd. Wielość rozwiązań w zakresie sposobu, miejsca i narzędzia prowadzenia wojen w pełni uzasadnia pogląd, że definiowanie wojny, wraz z jej ontologią i naturą oraz komponentami i mechanizmami jest niezbędne. Punktem wyjścia tej części dyskursu jest próba pochylenia się nad kluczową kategorią terminologiczną niniejszego rozdziału, jaką jest *„power”* z uwzględnieniem deskrypcji i eksplanacji. Patrząc przez optykę kwestii tłumaczeniowych, jak również kontekstualnych na uwagę zasługuje fakt, że zakres semantyczny tego terminu nie jest obcy znawcom literatury przedmiotu, szczególnie na trójstyku politologii, socjologii oraz stosunków międzynarodowych. Termin ten w swobodnym tłumaczeniu oznacza „siłę”, „władzę”, „potęgę”, odzwierciedlając tym samym, przy pomocy określonych wskaźników, możliwości ekonomiczne, polityczne, kulturowe czy militarne państwa, unii państw, regionu czy korporacji biznesowej.

Na potrzeby niniejszego opracowania warto sięgnąć po kategorię „władzy”, tak bliską przytaczanym tutaj rozważaniom M. Castellsa, który kładł nacisk na pierwiastek relacyjny, rozumiany jako zakres oddziaływania jednego podmiotu na drugi[34]. Na tej podstawie ma miejsce krystalizacja terminologii, w której *„power”* definiuje się jako zdolność państwa lub terytorium do bezpośredniego lub pośredniego wpływania na zachowania innych państw, podmiotów niepaństwowych oraz przebieg wydarzeń międzynarodowych”[35]. Istotę a zarazem specyfikę *„power”* odnaleźć można również w zbiorach encyklopedycznych i leksykalnych, w świetle których termin ten oznacza „(...)

[33] Ł. Roman, *Interdyscyplinarny wymiar polemologii*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej”, nr 1/2012, s. 186.
[34] Zob. M. Lisewski, *Soft...*, s. 45.
[35] Tamże, s. 45.

panowanie, władzę, wpływ na innych, zdolność do działania w celu osiągnięcia zamierzonego skutku, (...) polityczną kontrolę i wpływy”[36].

Analizując dostępne opracowania na uwagę zasługuje fakt, że sięgając po kategorię *„sharp power”* odnotować można szerokie spektrum działań, powszechnie znanych jako perswazja manipulacyjna, zmierzająca do zaprezentowania rzeczywistości taką, jaką ma być odbierana. Na naszych oczach dokonuje się działań określanych jako „(...) agresywne działania państwa prowadzone (...) w celu manipulacji wizerunkiem danego kraju (lub innego podmiotu stosunków międzynarodowych) bądź dla destabilizacji jego systemu społeczno-politycznego, bądź wymuszenia określonego postępowania jego władz”[37]. Spoglądając na warsztat Manuela Castellsa można z niemal stuprocentową pewnością powiedzieć, że mamy do czynienia z rzeczywistością zaprogramowaną, możliwą do uchwycenia za pomocą aparatu sieciowego. „Z tej perspektywy (*„sharp power”* – tu autor: D.B.) wykorzystuje perswazję, a konkretnie manipulację, jednak nie po to (...), aby uatrakcyjnić swój poziom, ale obniżyć atrakcyjność konkurenta”[38]. Działania, o których mowa wpisuje się w obraz współczesnych bitew o umysł, w obrębie których w sferze informacyjnej dokonuje się próba przejęcia kontroli nad społeczeństwem na drodze manipulacji, dezinformacji i propagandy.

Sharp power w konflikcie hybrydowym na przykładzie polsko-białoruskiego kryzysu migracyjnego

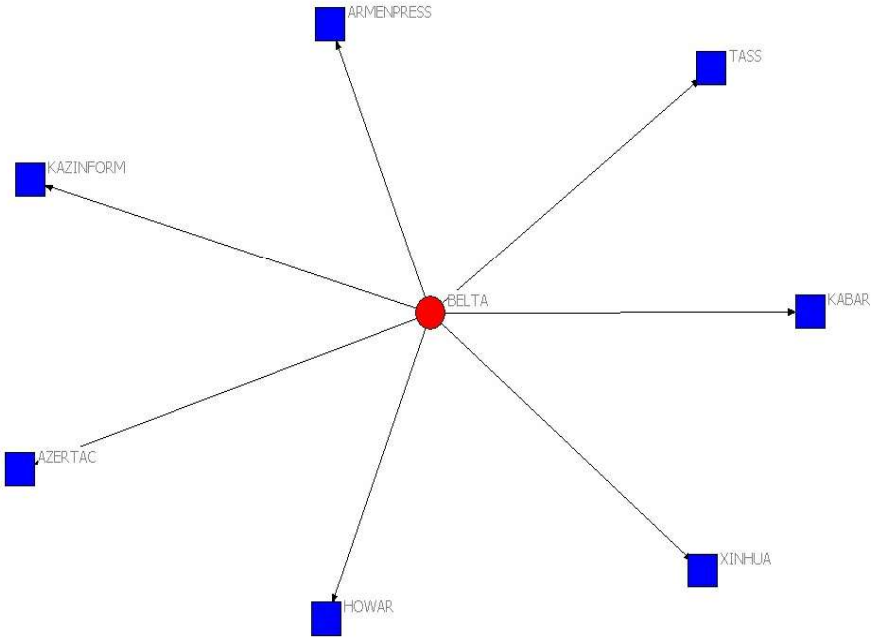
Zainicjowany w 2021 roku kryzys migracyjny na granicy polsko-białoruskiej był między innymi, podsycaną przez Kreml, odpowiedzią Mińska na ogólnoeuropejski sprzeciw wobec wyniku wyborów na urząd prezydenta Republiki Białorusi. Operacja „Śluza” ukierunkowana została na dwa elementarne cele: wewnętrzny, polegający na czerpaniu zysków z nielegalnej migracji, które trafiają do aparatu władzy i powiązanych z nim instytucji; zewnętrzny, polegający na destabilizacji struktur Unii Europejskiej i Paktu Północnoatlantyckiego z naciskiem na osłabienie pozycji oraz wizerunku tych podmiotów, wzmocnienie społecznych i politycznych antagonizmów w obrębie państw członkowskich

[36] Zob. E. Panas, *Soft power transnarodowych organizacji społeczeństwa obywatelskiego*, Lublin 2021, s. 22.
[37] Ł. Skoneczny, B. Cacko, *Sharp*..., s. 106.
[38] M. Lisewski, *Soft*..., s. 75.

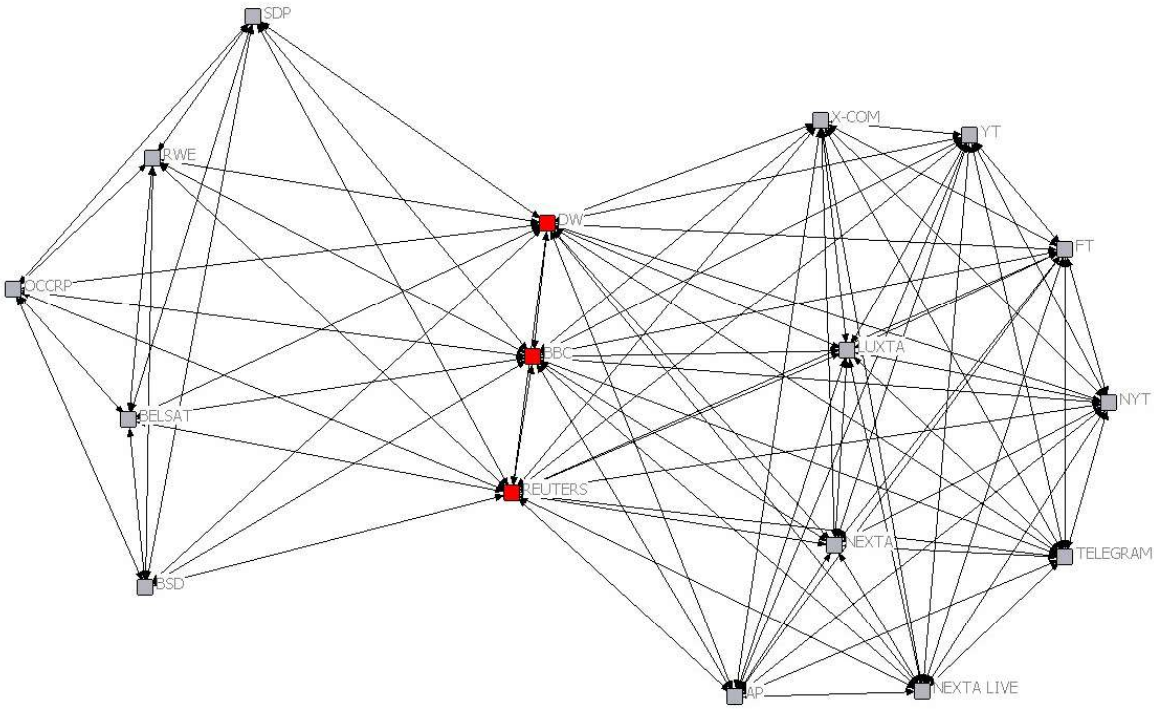
Unii Europejskiej czy próbę odwrócenia uwagi od przygotowania Federacji Rosyjskiej do pełnowymiarowej wojny z Ukrainą.

Istotną podbudową operacji „Śluza" jest szerokie spektrum działań wykraczających poza operację nielegalnej migracji, zwanej również „bronią D", a mających odzwierciedlenie w sferze informacyjno-psychologicznej. Mowa w tym miejscu o zdominowaniu białoruskiej i rosyjskiej przestrzeni medialnej przez materiały, będące głosem oskarżenia o uprzedzenia na tle rasowym, o niehumanitarne traktowanie migrantów i inne praktyki, wykraczające poza kodeks etyki i prawa człowieka. Przykładem prołukaszenkowskiej propagandy jest między innymi oficjalny przekaz insynuujący odpowiedzialność za kryzys humanitarny po stronie polskich służb mundurowych, które jakoby przerzucają na białoruską stronę granicy zwłoki migrantów, wyłaniających się wiosną na skutek pojawienia się roztopów, itd.[39]. Podbudową tego rodzaju narracji jest również przekaz o rzekomej próbie ataku ze strony Polski na Republikę Białorusi. W opinii Aleksandra Łukaszenki rząd państwa polskiego, przy współudziale Unii Europejskiej dąży do usunięcia prezydenta Białorusi, zaś działania na granicy polsko-białoruskiej stanowią preludium to zaplanowanego – zdaniem A. Łukaszenki – ataku ze strony państw Europy Zachodniej. W opinii władz Mińska wszelkie protesty oraz inne działania prodemokratyczne zostały zainspirowane i moderowane przez Polskę, Litwę, Czechy i inne[40]. Na łamach białoruskich mediów, w tym sieci Internetu (ryc. 1-3), dostrzec można narrację, obarczającą Rzeczpospolitą Polską oraz Unię Europejską za trudną sytuację na granicy. „Dziś cały świat jest świadkiem nieludzkiego traktowania migrantów przez Polaków. (...). Pod adresem Białorusinów napływają słowa wdzięczności ze strony narodu kurdyjskiego za wsparcie dla uchodźców"[41]. Wypowiedzi tej wtóruje kolejny komentarz przypisujący Zachodowi bestialskie zachowania wobec migrantów – „Jesteśmy porażeni tym, jak się zachowują polscy i litewscy pogranicy, tym, jak władze w Brukseli próbują nie zauważyć cynicznego stosunku do tych ludzi (to jest: uchodźców – tu: D.B.) ze strony władz państw członkowskich UE"[42].

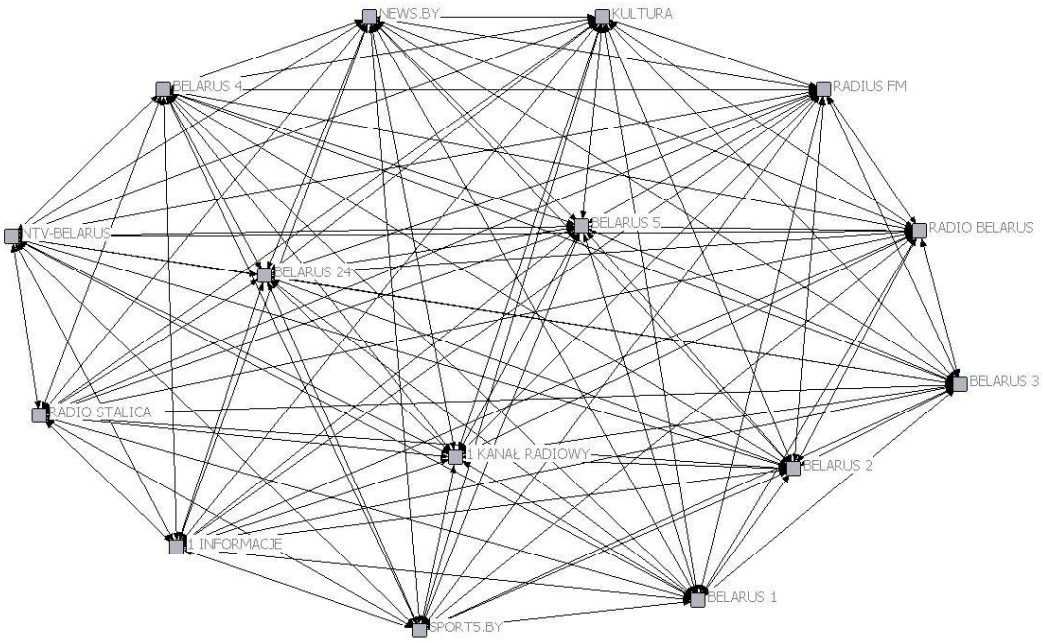
[39] https:/mlyn.by/23042024/beloruskkie-voennye-prorvali-graniczu-s-polshej-komu-nuzhen-provokaczionnyj-fejk/, data dostępu: 25.07.2025.
[40] https:/tass.ru/mezhdunarodnaya-panorama/9360531/, data dostępu: 25.07.2025.
[41] www.tvr.by/news/obshchestvo/r_aloyan_o_krizise_na_belorussko_polskoy_granitse/, data dostępu: 25.07.2025.
[42] www.tvr.by/videogallery/informatsionnoananaliticheskie/panorama/, data dostępu: 25.07.2025.



Ryc. 1. *Sieć (gwiazda) publicznych podmiotów medialnych tj. agencji prasowych*
Źródło: *opracowanie własne za pomocą Ucinet 6.232. i NetDraw*



Ryc.2. *Sieć powiązań instytucji medialnych skupionych wokół platform BELSAT i NEXTA*
Źródło: *Opracowanie własne za pomocą Ucinet 6.2.32. i NetDraw*



Ryc. nr 3. *Sieć powiązań białoruskich mediów państwowych*
Źródło: *opracowanie własne za pomocą Ucinet 6.232. i NetDraw*

Propagandowa tuba Mińska nakreśla granicę oraz pogranicze polsko-białoruskie w kategoriach ziemi obiecanej, w świetle której obywatele państwa polskiego wołają o pomoc ze strony Republiki Białorusi. „Zobaczcie co się dzieje z sąsiadami (...). Oni byli tacy zamożni (...). I gdzie teraz są? Stoją przy granicy i proszą, byśmy ich wpuścili na Białoruś. Żeby mogli przynajmniej kupić kaszę gryczaną. (...). Soli nie mają. Proszą nas o sól”[43].

W zakresie działań, wpisujących się w pakiet *„sharp power”* jest również propagandowy przekaz z udziałem Emila Czeczko – dezerterującego żołnierza Polski, który w opinii Mińska był zmuszany do działań niezgodnych z prawami człowieka, adresowanych do migrantów obecnych na polskiej granicy wschodniej[44]. Co więcej, odpowiedzialność za stan faktyczny na granicy przypisuje polskim służbom A. Łukaszenka, zdaniem którego

[43] www.ekhokavkaza.com/a/31827220/, data dostępu: 25.07.2025.
[44] Zob. więcej: B. Wypartowicz, W. Kozioł, *Między Bugiem a prawdą. Czy Polska może odbudować swoje wpływy na wschodzie*? , Warszawa 2024, s. 116.

Straż Graniczna państw, które nie chcą przepuszczać migrantów, (...) krzywdzi przybyszy, w przeciwieństwie do pomagających pograniczników białoruskich”[45].

Istotnym elementem niniejszych rozważań, dopełniającym mechanizm *„sharp power”* jest analiza sieci społecznych, przeprowadzona przy pomocy programu Ucinet i NetDraw, na bazie których przygotowano macierze danych, a następnie wizualizacje odwzorowujące sieć powiązań konglomeratów medialnych, zaangażowanych w politykę *„soft power”*. Dane do macierzy zagregowano za pomocą liczb (0, 1, 2, 3, itd.) w sposób umożliwiający nakreślenie struktury powiązań świata mediów Mińska i Kremla, w tym mniej lub bardziej sterowalnych ośrodków (czwartej) władzy. Rycina nr 1 obrazuje sieć o konfiguracji gwiazdy, w której najlepszą pozycję posiada węzeł Belta (stopień węzła, n=7,0), co przedkłada się na możliwość bezpośredniej kontroli na pozostałymi węzłami, których stopień wynosi 1 (n=1,0). Co więcej każdy węzeł o stopniu n=1,0 może wchodzić w relacje z innymi węzłami tej sieci tylko przy udziale, czy raczej za pośrednictwem węzła Belta. W przypadku struktury na rycinie nr 2 warto podkreślić kluczowe znaczenie aktorów (węzłów) takich jak: DW, Reuters, BBC, pełniących funkcję brokerów sieci, dla których stopień węzła n=16,0. Pozycja zajmowana przez węzły BBC, DW, Reuters gwarantuje stabilność struktury, z kolei ich wyłączenie ze struktury prowadzi do rozpadu całej sieci. Na uwagę zasługuje fakt, że analizowana struktura przybiera topologię „siatki”, co oznacza, że pozbawiona jest odizolowanych węzłów. Co więcej, aktorzy oznaczeni kolorem czerwonym (ryc. nr 2) stanowią rdzeń sieci, z kolei pozostałe węzły (np. Belsat, RWE n=7,0; Telegram, Nexta Live n=11,0) posiadają taką samą, niejako „zastępowalną” pozycję w strukturze, a tym samym ich „wyłączenie” z sieci nie zaburza funkcjonowania całej struktury. Rycina nr 3 odwzorowuje sieć o konfiguracji „siatki” oplatającą białoruski system medialny, w której każdy z 15-tu węzłów dysponuje analogiczną kompozycją relacji, w której stopień węzła wynosi 14,0 (n=14 – ryc. nr 3).

Warto podkreślić, że wysiłki podejmowane przez rosyjski i białoruski aparat władzy nie „zaowocowały” założonymi skutkami, przeciwnie – społeczeństwo europejskie okazało się odporne na dezinformacyjną politykę Mińska i Kremla, a europejskie służby i elity świata polityki – świadome zagrożeń, opracowały skuteczny sposób reagowania na

[45] Belta, serwis Telegram, 25.07.2025.

tego rodzaju zdarzenia. Z drugiej strony od momentu wybuchu zagrożenia w przestrzeni społecznej utrzymują się określone poglądy i nastroje społeczne wobec migrantów oraz polityki wewnętrznej i zewnętrznej państwa polskiego. Za możliwością ubiegania się o azyl przez migrantów z granicy polsko-białoruskiej opowiada się 19% respondentów, przeciwnego zdania jest 73% badanych – dla porównania w 2021 roku odsetek zwolenników azylu wynosił 33%, za przeciwników – 52%[46]. Postulat zwiększenia możliwości użycia broni palnej przez funkcjonariuszy wojska, policji i Straży Granicznej, broniących polskiej granicy wschodniej popiera 84% respondentów, wobec 11% wyrażających sprzeciw[47]. Politykę zamknięcia wszystkich przejść granicznych na odcinku granicy polsko-białoruskiej aprobuje 72% badanych, zaś co piąta osoba jest przeciwnego zdania[48]. Poruszając się wokół problematyki bezpieczeństwa oraz świadomości zagrożeń na uwagę zasługuje fakt, że 86% ankietowanych aprobuje program „Tarcza Wschód" w ramach którego polsko-białoruski i polsko-rosyjski odcinek granicy jest umocniony, zaś 39% jest zwolennikiem zastosowania tzw. pól minowych przy wspomnianych odcinkach granicy[49]. Pomimo nasilających się działań manipulacyjnych i dezinformacyjnych, dyskredytujących działalność służb granicznych na przestrzeni lat 2021-2025 utrzymuje się dość wysoka ocena pracy funkcjonariuszy Straży Granicznej, oscylująca w przedziale 60-85%[50].

Polityka *„sharp power"* związana z sytuacją na granicy polsko-białoruskiej rzutuje również na społeczny odbiór imigrantów i bezpośredni do nich stosunek. W świetle danych zagregowanych przez Centrum Badania Opinii Społecznej określenie „imigrant" wzbudzało negatywny stosunek wśród 39% badanych i najczęściej kojarzyło się z kimś, kto potrzebuje pomocy , jest uchodźcą wojennym lub politycznym (24%), kto szuka lepszych perspektyw na życie (22%), kto nielegalnie przekracza granice (6%) oraz niesie

[46] J. Scovil, *O sytuacji na granicy polsko-białoruskiej*, Komunikat z badań nr 81/2024, CBOS https://www.cbos.pl/SPISKOM.POL/2024/K_081_24.PDF, s. 2, data dostępu: 24.07.2025.
[47] Tamże, s. 3.
[48] Tamże, s. 5.
[49] J. Scovil, *O wojnie w Ukrainie i sytuacji na granicy wschodniej, Komunikat z badań nr 67/2024, Centrum Badań Opinii Społecznej*, s. 5-6, https://www.cbos.pl/SPISKOM.POL/2024/K_067_24.PDF, data dostępu: 25.07.2025.
[50] M. Kawalec, I. Gwiazda, *Ocena instytucji publicznych w marcu*, Komunikat z badań 28/2025, Centrum Badania Opinii Społecznej, s. 16, https://www.cbos.pl/SPISKOM.POL/2025/K_028_25.PDF, data dostępu: 25.07.2025.

za sobą niebezpieczeństwo lub kłopoty (6%)[51]. Patrząc przez pryzmat postrzegania obecności migrantów w Polsce warto zauważyć, że zdaniem 69% respondentów obcokrajowcy nadmiernie obciążają socjalne wydatki, w opinii 66% migranci przyczyniają się do wzrostu przestępczości w Polsce, zaś dla 55% badanych obniżają stawki godzinowe za wykonywaną pracę[52]. Zdaniem co dziesiątego respondenta w Polsce możliwość osiedlenia się powinna mieć każda osoba, z kolei niespełna co trzeci badany akceptuje osiedlanie się osób, które uciekają przed różnego rodzaju zagrożeniami[53].

Zakończenie

Przeprowadzona powyżej analiza *„sharp power”* wpisuje się w szeroko zakrojony dyskurs na temat zmian, jakie mają miejsce na płaszczyźnie geopolitycznej i odnoszą się do struktury oraz dynamiki konfliktów niekinetycznych. Co ważne, dokonują transformacji pola walki a zarazem dywersyfikacji źródeł i narzędzi stosowanych na tym polu. Warto podkreślić, że realizacja *„sharp power”*, w tym skala oraz natężenie determinowana jest zdolnościami do mobilizacji i partycypacji zasobów, kluczowych z punktu widzenia polityki *„soft power”*. Na kanwie powyższej analizy warto uwypuklić kilka wniosków:

- po pierwsze, kategoria *„sharp power”* jest bardzo pojemną kategorią analityczną, z kolei podejście sieciowe nie tylko uzupełnia lukę badawczą, ale otwiera również nowe pole eksploracji w tym zakresie;

- po drugie, przekaz medialny, szczególnie dezinformacja i propaganda nie dokonały zakładanego przez Mińsk i Moskwę rezonansu w społeczeństwie polskim. Przeciwnie, wedle przeprowadzonych badań ogólnopolskich Polacy mają świadomość zagrożeń na wschodniej granicy UE, wskazując nie tylko podmioty odpowiedzialne za te zagrożenia, ale opowiadając się za wyraźnym wzmocnieniem granicy (86% aprobuję Tarczę Wschód, 72% opowiada za zamknięciem granicy) i aprobatą dla działalności Straży Granicznej (85% pozytywnie ocenia pracę funkcjonariuszy SG, zaś 84% popiera użycie broni przez funkcjonariuszy);

[51] J. Scovil, *Skojarzenia Polaków ze słowem „imigrant”,* Komunikat z badań nr 30/2025, Centrum Badania Opinii Społecznej, s. 2 i 5, https://www.cbos.pl/SPISKOM.POL/2025/K_030_25.PDF, data dostępu: 25.07.2025.
[52] B. Roguska, *Postrzegana i postulowana obecność cudzoziemców w Polsce*, Komunikat z badań nr 31/2025, Centrum Badania Opinii Społecznej, s. 6, https://www.cbos.pl/SPISKOM.POL/2025/K_031_25.PDF, data dostępu: 25.07.2025.
[53] Tamże, s, 11.

- po trzecie, instrumenty w postaci manipulacji i dezinformacji w dalszym ciągu będą systematycznie stosowane przez reżim białoruski, co ma związek ze scentralizowaną strukturą powiązań medialnych w Republice Białorusi – sieć typu „gwiazda", w której agencja „Belta" pełni rolę kontrolera przekazu, w tym wszelkich przepływów (np. informacji) oraz powiązań z innymi podmiotami sieci państwowych instytucji medialnych Mińska;

- po czwarte, przeprowadzona analiza uwypukla dość silną sieć powiązań platformy Nexta (ryc. 2), skupiającą rozmaite międzynarodowe platformy komunikacji, w tym BBC czy Reuters pełniące rolę brokerów w przepływach i powiązaniach tej sieci. Sieć ta wykazuje również wyraźną asymetrię pomiędzy strukturami powiązań węzłów Belsat i Nexta.

W kontekście wniosków wynikających z rozważań prowadzonych na kanwie powyższego materiału warto podkreślić praktyczny pierwiastek analizy. Celem artykułu jest, z jednej strony nakreślenie zmian, jakie mają miejsce w obszarze konstruowania władzy, to jest w świecie sieci powiązań i przepływów, z drugiej stanowią próbę sformułowania ogólnych wniosków na temat stosowania mechanizmów oraz zasobów *„sharp power"*. Wytycznym oraz wnioskom wypływającym z przeprowadzonej analizy przypisać można charakter pragmatycznych wskazówek wykorzystania elementów *„sharp power"* w szeroko rozumianej geopolityce sieciowej.

References

Barney D., *Społeczeństwo sieci*, Wydawnictwo Sic!, Warszawa 2008.

Castells M., *Koniec Tysiąclecia*, Wydawnictwo Naukowe PWN, Warszawa 2009.

Castells M., *Władza komunikacji*, Wydawnictwo Naukowe PWN, Warszawa 2013.

Clausewitz C., *O wojnie*, Wydawnictwo Bellona, Lublin – Zamość 1995.

Foucault M., *Nadzorować i karać*, Wydawnictwo Aletheia, Warszawa 2006.

Kubiak W., *Władza*, [w:] *Encyklopedia socjologii*, tom 4, Oficyna Naukowa, Warszawa 2005.

Lisewski M., *Soft power, sharp power, linking power. Mocarstwowe sposoby działania Chin i ich znaczenie dla świata*, Wydawnictwo Adam Marszałek, Toruń 2021.

Muraszkiewicz M., *Esej: nowy paradygmat, czyli od systemu do sieci*, [w:]
B. Sosińska-Kalata i inni (red.), *Od informacji naukowej do technologii społeczeństwa komunikacyjnego*, Wydawnictwo SBP, Warszawa 2005.

Panas E., *Soft power transnarodowych organizacji społeczeństwa obywatelskiego*, Wydawnictwo UMCS, Lublin 2021.

Roman Ł., *Interdyscyplinarny wymiar polemologii*, „Obronność – Zeszyty Naukowe Wydziału Zarządzania i Dowodzenia Akademii Obrony Narodowej", nr 1/2012, s. 183-192.

Skoneczny Ł., Cacko B., *Sharp power – wprowadzenie do problematyki*, „Przegląd Bezpieczeństwa Wewnętrznego", nr 13/2021, s. 102-119.

Sozański T., *Sieć społeczna*, [w:] *Encyklopedia Socjologii*, tom 4, Oficyna Naukowa, Warszawa 2005.

Stoessinger J. G., *The Might of Nation. World Politics in Our Times*, McGraw-Hill, New York, 1969

Sułek M., Szymala E., *Potęga państw 2025. Ranking potęgometryczny*, Instytut Nowej Europy, Warszawa 2025.

Szacki J., *Historia myśli socjologicznej*, Wydawnictwo Naukowe PWN, Warszawa 2004.

Sztompka P., *Socjologia. Analiza społeczeństwa*, Wydawnictwo Znak, Kraków 2002.

Urry J., *Socjologia mobilności*, Wydawnictwo Naukowe PWN, Warszawa 2004.

Wypartowicz B., Kozioł W., *Między Bugiem a prawdą. Czy Polska może odbudować swoje wpływy na wschodzie?* , Wydawnictwo Prześwity, Warszawa 2024.

J. Scovil, *O sytuacji na granicy polsko-białoruskiej*, Komunikat z badań nr 81/2024, CBOS https://www.cbos.pl/SPISKOM.POL/2024/K_081_24.PDF, s. 2, data dostępu: 24.07.2025.

J. Scovil, *O wojnie w Ukrainie i sytuacji na granicy wschodniej*, Komunikat z badań nr 67/2024, Centrum Badań Opinii Społecznej, https://www.cbos.pl/SPISKOM.POL/2024/K_067_24.PDF, data dostępu: 25.07.2025.

M. Kawalec, I. Gwiazda, *Ocena instytucji publicznych w marcu*, Komunikat z badań 28/2025, Centrum Badania Opinii Społecznej, https://www.cbos.pl/SPISKOM.POL/2025/K_028_25.PDF, data dostępu: 25.07.2025.

J. Scovil, *Skojarzenia Polaków ze słowem „imigrant"*, Komunikat z badań nr 30/2025, Centrum Badania Opinii Społecznej, https://www.cbos.pl/SPISKOM.POL/2025/K_030_25.PDF, data dostępu: 25.07.2025.

B. Roguska, *Postrzegana i postulowana obecność cudzoziemców w Polsce*, Komunikat z badań nr 31/2025, Centrum Badania Opinii Społecznej, https://www.cbos.pl/SPISKOM.POL/2025/K_031_25.PDF, data dostępu: 25.07.2025.

Belta, serwis Telegram, data dostępu: 25.07.2025.

https:/mlyn.by/23042024/beloruskkie-voennye-prorvali-graniczu-s-polshej-komu-nuzhen-provokaczionnyj-fejk/, data dostępu: 25.07.2025.

https:/tass.ru/mezhdunarodnaya-panorama/9360531/, data dostępu: 25.07.2025.

www.tvr.by/news/obshchestvo/r_aloyan_o_krizise_na_belorussko_polskoy_granitse/, data dostępu: 25.07.2025.

www.tvr.by/videogallery/informatsionnoananaliticheskie/panorama/, data dostępu: 25.07.2025.

www.ekhokavkaza.com/a/31827220/, data dostępu: 25.07.2025.

„dot.pl" - czasopismo Rejestru domeny .pl

State Surveillance in Serbia: Examining the Role of Chinese-Supplied Surveillance Cameras

"They are increasing the capacity quite significantly. If this was deployed to Belgrade, it would indicate a level of camera density rarely seen outside of China".[1]

Tal Pavel
Legal Sciences, "Dunarea de Jos" University of Galati, Romania
ORCID: https://orcid.org/0000-0002-4046-0867
E-mail: Tal@cybureau.org

Received: 25.11.2025
Accepted: 25.11.2025
Published: 25.11.2025

Cite this article as:
T. Pavel, "*State Surveillance in Serbia: Examining the Role of Chinese-Supplied Surveillance Cameras*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/ 214711

Corresponding author:
Tal Pavel, University of Galati, Romania
E-mail: Tal@cybureau.org

Abstract

Objective – To examine Serbia's deployment of Chinese-supplied surveillance technologies and assess the implications for democracy, privacy, and civil liberties in the context of Serbia's deteriorating freedom indices and EU accession aspirations.

Goal – To analyse the technological cooperation between China and Serbia in surveillance infrastructure, evaluate the transparency and accountability of Serbian institutions in implementing these systems, review the legal framework governing digital surveillance, and assess local and international responses to this deployment.

[1] Jelena Jankovic and Reid Standish, 'Leaked Files Reveal Serbia's Secret Expansion Of Chinese-Made Surveillance' [2025] Radio Free Europe/Radio Liberty <https://www.rferl.org/a/exclusive-safe-city-china-surveillance-huawei-facial-recognition/33501155.html>.

Methodology – This study employs a qualitative research approach based on document analysis from diverse, highly reliable sources. The methodology prioritises relevance, reliability, and diversity, integrating academic publications, reports from established human rights organisations, investigative journalism, and official government documents. The 46 sources were selected to ensure comprehensive coverage of technological, legal, political, and social dimensions of surveillance deployment in Serbia.
Findings – The research reveals that Serbia has significantly expanded its state surveillance capabilities through a strategic partnership with China, particularly with Huawei, deploying thousands of cameras equipped with facial and license plate recognition across major cities. The findings demonstrate a troubling lack of transparency and accountability, with agreements classified as confidential and explicit references to Chinese involvement deliberately obscured. Serbia's legal framework for digital surveillance remains underdeveloped, lacking adequate oversight mechanisms and privacy protections. Locally, concerns persist about the political misuse of surveillance for control rather than public safety. Internationally, the EU has expressed alarm over Chinese technological penetration and its implications for Serbia's EU accession goals.

Keywords: Serbia, Surveillance, Policy, China, Privacy

Introduction

Serbia's democracy has deteriorated over the past decade; the government, led by President Aleksandar Vučić, centralises power and influences state institutions, "steadily eroded political rights and civil liberties, putting pressure on independent media, the political opposition, and civil society organisations".[2] Multiple indices document a consistent decline in Serbia's general and press freedom. Freedom House labels Serbia as "Partly free" and indicates an ongoing deterioration in the freedom and democracy score, as represented in Table 1 ("Freedom House's Freedom Index").[3]

[2] Freedom House, 'Serbia: Freedom on the Net 2024' <https://freedomhouse.org/country/serbia/freedom-net/2024>.
[3] Freedom House, 'Serbia: Country Profile' <https://freedomhouse.org/country/serbia>.

Year	Freedom in the World Score (out of 100)	Democracy Score (out of 100)
2020	-	49.4
2021	64	48.21
2022	62	46.43
2023	60	46.43
2024	57	43.45
2025	56	-

Table 1: Freedom House's Freedom Index

Reporters Without Borders' Press Freedom Index indicates a constant deterioration in Serbia's position according to the 2022-2025 methodology: From "Problematic" (55-70 points) in 2022 and 2023 to "Difficult" (40-55 points) in 2024 and 2025, alongside ongoing deterioration in global score from 2020.[4]

Year	Position	Global Score	Press Freedom Status
2025	96	53.55	Difficult
2024	98	54.48	Difficult
2023	91	59.16	Problematic
2022	79	61.51	Problematic
2021	93	67.97	-
2020	93	68.38	-

Table 2: Reporters Without Borders' Press Freedom Index

The "Mapping Media Freedom" project, conducted by the European Centre for Press and Media Freedom, documented 10,773 media freedom incidents in 45 countries between 2014 and 2025. Analysing data on the number of incidents per country and the number of citizens in each country provides a multi-dimensional, fascinating insight into Serbia's position on press and media freedom.

Source of data

- European Centre for Press and Media Freedom – Columns "Country", "Number of Media Freedom Incidents".[5]
- Central Intelligence Agency (CIA) – Column "Number of Citizens".[6]

[4] Reporters Without Borders (RSF), 'World Press Freedom Index 2025' <https://rsf.org/en/index>.
[5] European Centre for Press and Media Freedom, 'Mapping Media Freedom' <https://www.ecpmf.eu/monitor/mapping-media-freedom/>.
[6] Central Intelligence Agency (CIA), 'Population Comparison - The World Factbook' <https://www.cia.gov/the-world-factbook/field/population/country-comparison/>.

- Authors' processing – Columns “Percentage of all Incidents”, “Rank – Number of Incidents”, “Incidents per Capita”, “Rank - Incidents per Capita”.

Country	Incidents			Citizens		
	Number of Media Freedom Incidents	Percentage of all Incidents	Rank – Number of Incidents	Number of Citizens	Incidents per Capita	Rank - Incidents per Capita
Serbia	566	5.25	7	6,652,212	0.0000851	4

Table 3: European Centre for Press and Media Freedom’s Mapping Media Freedom

Serbia's 7th place ranking in the number of media freedom incidents (566 incidents, 5.25% of total) is particularly alarming when considered proportionally. Serbia's population of approximately 6.7 million is substantially smaller than the six countries ranking above it. When incidents are normalised per capita, Serbia's media freedom violation density ranks 4th, among Europe's highest, suggesting systematic rather than isolated press freedom suppression.

Three independent human rights indices—Freedom House, Reporters Without Borders, and the European Centre for Press and Media Freedom—provide converging empirical evidence of Serbia's deterioration in democratic and media freedom. This is not a subjective assessment but a documented reality measured through different methodologies: declining freedom scores (from 64 to 56), worsening press freedom classification (from "Problematic" to "Difficult"), and exceptionally high media violation density (4th globally per capita). This deterioration establishes the critical context for understanding Serbia's surveillance deployment: a country experiencing democratic backsliding while simultaneously adopting Chinese surveillance technologies at densities "rarely seen outside of China".[7]

Literature Review

Existing studies on Serbia's digital sphere encompass multiple dimensions, yet critical gaps remain in understanding the intersection of surveillance technology, authoritarian governance, and foreign technology partnerships. This review synthesises current research, identifies theoretical frameworks, and articulates the specific contributions

[7] Jankovic and Standish (n 1).

this study makes to surveillance studies, authoritarian diffusion theory, and EU enlargement literature.

Digital Development in Serbia – Historical analyses provide important context for understanding Serbia's contemporary digital governance challenges. Tunnard (2003) examines the transformative period of the 1990s, analysing how communications and information systems shifted from state-controlled media to the relative "anarchy" of the Internet, and documenting early attempts by states to control digital information flows.[8] Steele (2024) investigates independent media development, specifically examining Radio B92's role in creating new media development models during Serbia's democratic transition.[9] Mihaljinac & Mevorah (2019) extend this historical narrative from 1996 to 2014.[10]

Digital Usage – Research on digital usage patterns provides demographic and socioeconomic context. Ćelić et al. (2018) analyse the Serbian customers' attitude toward Internet usage,[11] While Stojić (2017) examines digital adoption among elderly populations, revealing significant generational divides in technology access and literacy.[12] Gagić et al. (2016) and Stojić (2023) studied rural Internet penetration and e-business applications. Milovanovic (2015) documents uneven digital development across Serbia's urban-rural divide.[13]

Digital Sovereignty – Recent studies examining Serbia's digital sovereignty and information manipulation strategies. Simić et al. (2024) argue that Serbia employs "a

[8] Christopher R Tunnard, 'From State-Controlled Media to the "Anarchy" of the Internet: The Changing Influence of Communications and Information in Serbia in the 1990s' (2003) 3 Southeast European and Black Sea Studies 97 <https://www.tandfonline.com/doi/abs/10.1080/713999348>.

[9] Janet Steele, 'What Can We Learn From the Short History of Independent Media in Serbia? Radio B92, George Soros, and New Models of Media Development' (2024) 29 The International Journal of Press/Politics 646 </doi/pdf/10.1177/19401612231170092?download=true>.

[10] Nina Mihaljinac and Vera Mevorah, 'Broken Promises of Internet and Democracy: Internet Art in Serbia, 1996–2014' (2019) 41 Media, Culture & Society 889 </doi/pdf/10.1177/0163443719831177?download=true>.

[11] Đorđe Ćelić and others, 'Differences in Attitudes toward Internet Usage-Empirical Study from Serbia' (2018) 23 STRATEGIC MANAGEMENT 17.

[12] Gordana Stojić, 'Internet Usage by the Elderly in Serbia' (2017) 0 Facta Universitatis, Series: Philosophy, Sociology, Psychology and History 103 <https://casopisi.junis.ni.ac.rs/index.php/FUPhilSocPsyHist/article/view/2731>.

[13] Slavoljub Milovanovic, 'Application of Internet Technology and Electronic Business Concept in Serbia' (2015) 19 Procedia Economics and Finance 278 <https://www.sciencedirect.com/science/article/pii/S2212567115000283?via%3Dihub>.

common strategy of information manipulation to subvert any foreign or domestic authority other than the ruling party".[14] Others analyse various cyber threats[15] including cybercrime,[16] cyberbullying,[17] and threats to digital privacy.[18]

Regulatory Frameworks – Studies on Serbia's cyber regulations reveal significant gaps between legal frameworks and practice. Marković & Marković (2025) evaluate the existing general and Serbian legal mechanisms, their adaptability to contemporary technological threats, and their potential for reform.[19] Golić (2023) examines the normative framework for electronic administration,[20] while Kovačević et al. (2023) analyse the Serbian Computer Emergency Response Team's contribution to national security.[21]

Surveillance – The most directly relevant literature addresses state surveillance practices in Serbia. Manojlović et al. (2024), Milošević (2013), and Žarković et al. (2016) analyse the legal dimensions of public and covert monitoring, recording, and surveillance systems.[22] Veljkovic et al. (2024) examine the impact of secret data collection on privacy

[14] Dragan R Simić, Dragan Đukanović and Saša Mišić, 'Sovereignty in Cyberspace: The Case of Serbia Between "Digital Authoritarianism" and "Internet Freedom"' <https://rfpn.fpn.bg.ac.rs/handle/123456789/1444>.

[15] Nenad N Kovačević, Komazec Nenad and Antonio Mak, 'Analysis of the Impact and Actuality of Challenges, Risks and Threats to the Security of the Republic of Serbia' (2023) 20 Kultura Polisa 146.

[16] Lazar V Stošić, Aleksandra V Janković and Lazar Stošić, 'CYBERCRIME IN THE REPUBLIC OF SERBIA: PREVALENCE, SITUATION AND PERSPECTIVES' (2022) 19 KULTURA POLISA 82 <https://kpolisa.com/index.php/kp/article/view/1444>; Mirjana Pavlović, 'FIGHT AGAINST CYBERCRIME IN SERBIA - Achievements and Challenges'.

[17] Branislava Popović-Ćitić, Sladjana Djurić and Vladimir Cvetković, 'The Prevalence of Cyberbullying among Adolescents: A Case Study of Middle Schools in Serbia' (2011) 32 School Psychology International 412 </doi/pdf/10.1177/0143034311401700?download=true>; Bojan Veljkovic and others, 'CYBERBULLYING RESEARCH ON YOUTH POPULATION IN SERBIA' (2022) 7 RAP CONFERENCE PROCEEDINGS 72.

[18] Ivona Živković and Dalibor Petrović, 'Political (Ab)Use of the Internet- Facebook in Hands of Serbian Right-Wing' (2024) 66 Sociologija 64 <https://doiserbia.nb.rs/Article.aspx?ID=0038-03182401064Z>.

[19] Darko Marković and Darija Marković, 'CYBERCRIME AND LAW – MANAGING CHALLENGES AND PROSPECTS IN THE DIGITAL AGE' [2025] Pravo - teorija i praksa <https://casopis.pravni-fakultet.edu.rs/index.php/ltp/article/view/898/753>.

[20] Darko Golić, 'Normative Regulation of Electronic Administration in Republic of Serbia' (2023) 40 Pravo - teorija i praksa 44 <https://orcid.org/0000-0003-2315-5040>.

[21] Kovačević, Nenad and Mak (n 15).

[22] Milan Žarković, Zvonimir Ivanović and Ivan Žarković, 'Public Video Surveillance: A Puzzling Issue for Serbian Lawmakers.' (2016) 18 Varstvoslovje: Journal of Criminal Justice & Security 214 <https://openurl.ebsco.com/contentitem/gcd:116579650?sid=ebsco:plink:crawler&id=ebsco:gcd:116579650>; Milan Milošević, 'Legal Issues Regarding Secret Communication Surveillance In Serbia' (2013) 3 International Journal of Economics & Law 118 <https://www.ceeol.com/search/article-detail?id=40819>; Dragan Manojlović, Dejana Đorđić and Vojislav Jović, 'Legal Aspects of Secret Surveillance and Recording and Process Authorities for Its Implemenation: Comparative Research' (2024) 14 Civitas 188 <https://www.ceeol.com/search/article-detail?id=1306100>.

rights, while Budak et al. (2012) investigate Serbian citizens' attitudes toward privacy, data protection, surveillance, and security, finding that demographic characteristics significantly influence these attitudes.[23]

The current literature lacks a systematic analysis of China-Serbia technological cooperation in the deployment of Chinese surveillance cameras on Serbian streets. To minimise this research gap, the paper focuses on the following research question: (RQ1) What is the technological surveillance cooperation between China and Serbia? (RQ2) How transparent and accountable are Serbian state institutions in their deployment and usage of digital surveillance technologies? (RQ3) What is the legal framework for digital surveillance in Serbia? (RQ4) What is the local and foreign reaction to Serbia's digital surveillance?

Methodology

This study employs a qualitative document analysis approach using an exploratory case study design. Serbia serves as a critical case for understanding Chinese surveillance technology exports to European candidate countries, given its unique position as it navigates between EU accession aspirations and deepening partnerships with China amid documented democratic backsliding.

Data Collection and Source Selection – Data collection prioritised diverse, highly reliable sources based on three core principles: relevance (direct connection to research questions), reliability (recognised accuracy and methodological soundness), and diversity (multiple perspectives and source types).

A chronological timeline documented key events from 2009 to 2025, enabling the identification of critical junctures and deployment patterns. The final corpus comprised of 46 primary documents including: (1) Academic publications, (2) Reports from established Human Rights organisations including Amnesty International, Reporters Without Borders, Freedom House, and the European Centre for Press and Media Freedom, (3) Investigative journalism from reputable outlets, (4) Official government and

[23] Jelena Budak, Ivan-Damir Aniae and Edo Rajh, 'Public Attitudes towards Surveillance and Privacy in Western Balkans: The Case of Serbia' [2012] Radni materijali EIZ-a 5 <www.eizg.hr>.

parliamentary documents, (5) Primary documentation, including archived web pages and leaked documents.

Scope – This study focuses specifically on the bilateral technological surveillance cooperation between China and Serbia, examining the supply, deployment, and implications of Chinese-manufactured surveillance technologies within Serbian territory. The analysis is deliberately bounded to this particular Sino-Serbian partnership. It does not extend to China's surveillance technology exports to other countries or Serbia's potential surveillance-related cooperation with other states or technology providers.

Limitations – This study acknowledges several constraints: (1) reliance on documentary evidence limits access to lived experiences and classified information, (2) predominance of English-language sources may underrepresent Serbian domestic discourse, (3) many Sino-Serbian agreements remain classified, requiring reliance on leaked documents and investigative reporting, (4) some surveillance capability claims could not be independently verified, and (5) as a single case study, findings provide deep contextual understanding but may not be directly generalizable.

Findings

Serbia, which enjoys the most comprehensive relationship with China among the Western Balkan countries, was described as “the Focal Point of China’s 'Digital Silk Road'” and, since early 2009, has developed extensive and strategic relations with China, primarily focused on financial and infrastructure-related projects, but also extends into the national security domain and into technical cooperation in infrastructure.[24] In addition, a joint initiative involving the establishment of joint police patrols alongside

[24] Stefan Vladisavljev, ‘China’s “Digital SilkRoad” Enters theWestern Balkans’ (China Observers in Central and Eastern Europe(CHOICE) 2021) <https://chinaobservers.eu/wp-content/uploads/2021/06/CHOICE_policy-paper_digital-silk-road_A4_web_04.pdf>.

military collaboration.[25] Serbian security agencies deployed Chinese surveillance technologies for wider state control and repression directed against civil society.[26]

In 2011, the Serbian Ministry of the Interior and the Chinese technology company Huawei Technologies Co., Ltd. initiated negotiations for a potential upgrade of the Ministry's information and telecommunications system, utilising solutions designed to enhance citizens' overall security within the “Safe City” project. This project, however, would be highly intrusive for citizens.[27] A Memorandum of Understanding outlining the proposed cooperation and the next steps in implementing the project was signed in December 2014. In April 2017, the Ministry of Trade, Tourism and Telecommunications signed a contract with Huawei to build a broadband internet network in Serbia. The pilot phase of the “Safe City” project has commenced with the installation of new surveillance cameras that feature significantly higher resolution and advanced technical capabilities. Also, cameras will include facial recognition software.

In September 2018, both countries signed several agreements, including one signed by the Minister of Finance, “on the purchase of equipment, works and services for the realisation of a capital project of traffic surveillance”, from Huawei.[28]

As part of this agreement, in early 2019, Serbia launched the “Safe City” project in Belgrade, a two-year project of installing a thousand cameras, purchased from the Huawei to cover 800 locations in the capital, “enabling the face and licences plates recognition, making every citizen’s move known to the police”, as well as “patrol cars and

[25] Euronews, ‘Chinese Police to Help Serbia Cope with Its Workers, Tourists’ <https://www.euronews.com/2019/08/02/chinese-police-to-help-serbia-cope-with-its-workers-tourists>.

[26] Amnesty International, ‘Serbia: “A Digital Prison”: Surveillance and the Suppression of Civil Society in Serbia’ (2024) <https://www.amnesty.org/en/documents/eur70/8813/2024/en/>.

[27] SHARE Fondacija, ‘New Surveillance Cameras in Belgrade: Location and Human Rights Impact Analysis – “Withheld”’ <https://sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/>.

[28] B92, ‘Serbia and China Sign Several Important Documents’ <https://www.b92.net/o/eng/news/business?yyyy=2018&mm=09&dd=18&nav_id=105087>; Stefan Vladisavljev, ‘How Did Serbia and Huawei Cooperate: A Chronology’ [2019] BFPE <https://en.bfpe.org/in-focus/region-in-focus-focus/how-did-serbia-and-huawei-cooperate-a-chronology/>; Vuk Vuksanovic, ‘Securing the Sino-Serbian Partnership’ [2019] Chinaobservers <https://chinaobservers.eu/securing-the-sino-serbian-partnership/>.

police officers in the street will gradually become equipped with these cameras" to increase public safety and facilitate the fight against crime.[29]

In April 2019, Deputy Prime Minister and Minister of Trade, Tourism and Telecommunications, Rasim Ljajić, signed in Beijing the Memorandum of Understanding for the "Smart Cities'' project, positioning Huawei as a strategic partner of the Serbian Government for the development of the smart cities strategy in Belgrade, Niš, and Novi Sad. In addition, Serbia has installed surveillance cameras across the countryside through contracts with the local company, Macchina Security, which have taken place under the radar, utilising cameras from the China-based Dahua company, a U.S. government-sanctioned entity and one of the world's largest manufacturers of video surveillance technology.[30] For example, Osecina, a small town in western Serbia, has only 2,700 people and one installed camera for every 100 inhabitants.[31]

Leaked documents reveal new contracts from March 2024 for software and services designed to enhance Serbia's private police-only Huawei industry eLTE private network solution,[32] which supports facial and license plate recognition and could enable up to 3,500 surveillance cameras. Others note that the Serbian government is installing approximately 8,000 Huawei surveillance cameras with facial recognition capabilities, with thousands already deployed in the capital.[33]

The Serbian government significantly expanded its Chinese-made "Safe City" surveillance program, despite public protests and legal concerns in Serbia and beyond.

Privacy – Risk of misuse of the smart surveillance cameras for political purposes[34]. The Commissioner for Public Information and Protection of Personal Data between the years

[29] SHARE Fondacija (n 27).
[30] Johana Bhuiyan, 'Dahua Facial Recognition Touts "Real-Time Uighur Warnings"' [2021] Los Angeles Times <https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur>.
[31] Natalija Jovanovic, 'How Serbia Became Blanketed In Chinese-Made Surveillance Cameras' [2023] Radio Free Europe/Radio Liberty <https://www.rferl.org/a/serbia-surveillance-cameras-china/32526515.html>.
[32] 'Industry eLTE Private Network Solution' (*Huawei Enterprise*) <https://e.huawei.com/en/solutions/enterprise-wireless/industry-wireless/industrial-elte-private-network> accessed 3 November 2025.
[33] Jankovic and Standish (n 1); Jovanovic (n 31).
[34] The Prague Security Studies Institute, 'The Sum of All Fears – Chinese AI Surveillance in Serbia' (2020) <https://www.pssi.cz/wp-content/uploads/2025/07/8447_the-sum-of-all-fears-chinese-ai-surveillance-in-serbia.pdf>.

2004-2018, Rodoljub Sabic, said, “In the country in which the regime has used personal data against its citizens many times, video surveillance looks more like a new way of control than a new way of increasing safety”. Following reports from 2022 indicated that few days after plainclothes bystanders took pictures with unusual high-resolution technology looking similar to Huawei’s Intelligent Large-Screen Handheld “Huawei EP 821 trunking terminal” dozens of fines issued for obstructing traffic, apparently without any “stop and identify” procedure, the current commissioner, Milan Marinovic, was tasked with looking into breaches of personal data and whether facial-recognition capabilities were used at the protests.[35]

Accountability – Lack of transparency and accountability of the signed agreements, even labelled ‘confidential’, including avoiding explicit citation of Huawei as a supplier. The webpage on the Huawei website, which described, as of August 2018, their involvement in Serbia’s “Safe City” project, disappeared after Human rights researchers filed Freedom of Information requests and alerted the Serbian public.[36] Moreover, in its past statements, Huawei has maintained that it is only a manufacturer and vendor and that responsibility for how its technology is used ultimately lies with the user.

Due to inadequate Serbian legal regulation and a lack of regulations governing video surveillance, the local government lack a clear mandate to utilise surveillance systems.[37] Three years after it began installing smart cameras in Belgrade, the government decided it was time to find legal grounds for their deployment, only to withdraw its legislative efforts following intense public pressure.[38]

---

[35] Commissioner for Information of Public Importance and Personal Data Protection, ‘The Commissioner Conducts Supervision Procedure in Ministry of Interior, Regarding Suspicion of Facial Recognition Technology Use’ <https://tinyurl.com/3ub2bnez>.

[36] Danilo Krivokapić, ‘Starting the Debate on Facial Recognition: A Case Study from Belgrade’ (Share Foundation 2022); Huawei Enterprise, ‘Huawei Safe City Solution: Safeguards Serbia’ <https://web.archive.org/web/20190313232443/https://e.huawei.com/en/case-studies/global/2018/201808231012>.

[37] The Prague Security Studies Institute (n 34).

[38] Jankovic and Standish (n 1); Jovanovic (n 31); Đorđe Krivokapić, ‘A Disturbing Marriage: Serbia and China Team Up on Digital Surveillance’ [2022] CEPA <https://cepa.org/article/a-disturbing-marriage-serbia-and-china-team-up-on-digital-surveillance/>.

“Presence of ‘Big Brother’ in Serbia” – The Chinese high-tech industries are required under the Chinese National Security Act to relay all data in their possession to Beijing’s intelligence service, in addition to the fact that such a surveillance project makes Serbia a laboratory for Chinese influence and projects and “a vital test case for Chinese surveillance infrastructure beyond its borders”.[39]

The EU – Such concerns were raised not only in Serbia but also in the EU. Since Serbia is a candidate for accession to the EU, the “Safe City” project raised national security concerns in the European Parliament about “China's penetration into Europe”, in a project where Huawei actively participates in more than 120 cities and more than 40 countries in the process of developing “Smart Cities”.

Although Huawei is a private company, the Chinese Communist Party has selected it as a national champion for developing homegrown telecom equipment. The US government has blacklisted the company over its connections to the Chinese military and concerns that its equipment could be used for espionage.[40] In October 2019, the European Parliament members Mara Bizzotto and Anna Bonfrisco raised the following questions: (1) Does it know the details of the “Safe City” project?, (2) Will it raise this issue urgently with the Serbian Government and ascertain whether EU funding is being used for the project? (3) Is this project not a case of dangerous Chinese interference in Europe’s politics, economy, freedom and security, and incompatible with Serbian accession to the EU?[41]

In June 2021, European Parliament member from France, Gwendoline Delbos-Corfield, claimed that “The European Parliament is taking a close look at China’s high-tech presence in Serbia, indicating that an official representative of Belgrade who told one of

[39] Mara Bizzotto and Anna Bonfrisco, ‘Parliamentary Question | Safe City Project in Serbia - China Penetrating into Europe’ <https://www.europarl.europa.eu/doceo/document/E-9-2019-003068_EN.html>; N1 Belgrade, ‘Thousand Surveillance Cameras in Belgrade – for Safety or Control?’ <https://web.archive.org/web/20190517113322/http://rs.n1info.com/English/NEWS/a456797/Belgarde-will-have-1-000-new-survillance-cameras.html>; Reid Standish, ‘Serbia’s Legal Tug-Of-War Over Chinese Surveillance Technology (Part 2)’ [2022] Radio Free Europe/Radio Liberty <https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32145138.html>; Vuksanovic (n 28).

[40] SHARE Fondacija (n 27).

[41] Bizzotto and Bonfrisco (n 39).

these parliamentary meetings that Belgrade would be the city ‘where every corner will be under surveillance’”.[42]

Discussion

This study examined Serbia's deployment of state surveillance cameras based on Chinese technology, focusing on questions of technological cooperation, transparency, legal frameworks, and reactions both locally and internationally. The findings enable answering the different research questions:

(RQ1) **Cooperation –** China and Serbia have developed multifaceted cooperation extending beyond financial and infrastructure projects to include significant security collaboration. This is exemplified by the "Safe City" project, a strategic joint initiative with Huawei, wherein thousands of Chinese-made surveillance cameras equipped with facial and license plate recognition capabilities have been installed in Belgrade and other major Serbian cities. This expansive deployment markedly increased the state's surveillance capacity, signalling a deeper technological alliance that integrates Chinese surveillance technology into Serbia's national security apparatus. The cooperation also includes police and military collaboration, reinforcing a broad security cooperation framework between the two states.

(RQ2) **Accountability –** The analysis reveals a troubling lack of transparency and accountability within Serbian state institutions regarding their use of digital surveillance technologies. Many of the agreements signed with Huawei and local partners have been classified as confidential, and even explicit references to Huawei’s involvement have been deliberately obscured. Serbian authorities have also struggled to establish clear legal frameworks regulating the use of such intrusive technologies, and attempts to formalise the legal grounds for camera deployment have been withdrawn following public backlash. This opacity, combined with inadequate regulatory oversight, raises significant concerns about accountability.

[42] Georgi Gotev, ‘MEPs Sound the Alarm over Chinese Mass Surveillance Project in Belgrade’ [2021] Euractiv <https://www.euractiv.com/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/>.

(RQ3) **Legality –** Serbia's legal framework for digital surveillance is underdeveloped and inadequate to regulate the use of advanced surveillance technologies. Existing laws do not provide clear mandates or comprehensive oversight mechanisms for the deployment and operation of facial recognition and other intrusive surveillance systems. This legal lacuna creates risks of privacy violations and abuse, particularly given the authoritarian governance trends and history of personal data misuse in Serbia. Attempts to introduce legal regulations have stalled under pressure from the public and civic society, reflecting tensions between technological expansion and civil rights protections.

(RQ4) **Reaction –** Locally, the deployment of Chinese surveillance technology has sparked significant concerns about privacy and human rights, with activists and former data commissioners warning that surveillance is being used as a tool of political control rather than for genuine public safety. Reports of misuse during public protests and concerns over data breaches have underscored local scepticism and alarm. Internationally, the European Parliament and the broader EU have expressed serious concerns about China's expanding high-tech footprint in Serbia. These concerns emphasise the risks of Chinese political interference, potential espionage, and the compatibility of such cooperation with Serbia's aspirations for EU accession. The US government's blacklist of Huawei further complicates these dynamics, highlighting geopolitical tensions surrounding the deployment of Chinese technology in Europe. This international scrutiny frames Serbia as a testing ground for Chinese surveillance projects beyond its borders.

Conclusions

This study has revealed that Serbia's deployment of Chinese-supplied surveillance cameras represents a significant expansion of state surveillance capabilities, enabled through a deepening technological and security partnership with China, notably Huawei. The "Safe City" initiative and related projects have created a level of surveillance capacity rarely seen outside China, substantially increasing the state's ability to monitor public spaces with advanced facial and license plate recognition technologies.

However, this expansion occurs amid troubling concerns regarding the transparency and accountability of Serbian state institutions, which have often classified agreements as

confidential and obscured Huawei's direct involvement. Moreover, Serbia's legal framework governing digital surveillance remains underdeveloped, lacking apparent oversight, regulatory mandates, and protections for privacy and civil rights. Public backlash has stalled legislative attempts to formalise legal bases for these surveillance tools.

Locally, there is widespread concern about potential abuses of the surveillance infrastructure for political control rather than genuine public safety. Internationally, the deployment has drawn scrutiny and criticism from the EU and other Western actors, who are concerned about Chinese political influence and strategic technology penetration in Europe. The combination of legal gaps, institutional opacity, and geopolitical tensions positions Serbia as both a testing ground and a vulnerability point in the broader contest over digital sovereignty and surveillance in the Balkans.

Future Research

Additional studies could examine (1) **Alternative Surveillance Systems** – other means of surveillance in Serbia, including local and foreign technologies. (2) **Civil Society Responses** – to the proliferation of surveillance technologies, including grassroots efforts such as the "thousand cameras" initiative, where citizens have catalogued and mapped hundreds of surveillance cameras across Belgrade.[43] (3) **Comparative Analysis of Chinese Surveillance Exports** – the geopolitical dimension, particularly concerning China's role as a global exporter of surveillance technologies and its implications for EU candidate countries. (4) **Democratic and Human Rights Impacts** – The long-term effects on democratic governance, media freedom, and human rights in Serbia, with a focus on how surveillance influences political opposition, press independence, and public trust. (5) **Legal Frameworks and Regulatory Gaps** – examine Serbia's evolving legal framework for digital surveillance in greater depth. (6) **Role of International Actors** – analysing the role of international actors in mitigating digital surveillance export to Western countries.

[43] hiljadekamera, 'European Promotion of the SHARE Foundation's Book on Biometric Surveillance' <https://hiljade.kamera.rs/en/>; 'Surveillance under Surveillance' <https://hiljade.kamera.rs/map/>.

References

Amnesty International, *Serbia: "A Digital Prison": Surveillance and the Suppression of Civil Society in Serbia*, 2024. https://www.amnesty.org/en/documents/eur70/8813/2024/en/

B92, "Serbia and China Sign Several Important Documents". https://www.b92.net/o/eng/news/business?yyyy=2018&mm=09&dd=18&nav_id=105087

J. Bhuiyan, *Dahua Facial Recognition Touts "Real-Time Uighur Warnings*, 2021, Los Angeles Times. https://www.latimes.com/business/technology/story/2021-02-09/dahua-facial-recognition-china-surveillance-uighur

M. Bizzotto, A. Bonfrisco, *Parliamentary Question | Safe City Project in Serbia - China Penetrating into Europe*. https://www.europarl.europa.eu/doceo/document/E-9-2019-003068_EN.html

J. Budak, I-D. Aniae I-D, E. Rajh, P*ublic Attitudes towards Surveillance and Privacy in Western Balkans: The Case of Serbia*, 2012, Radni materijali EIZ-a 5 www.eizg.hr

D. Ćelić at al., *Differences in Attitudes toward Internet Usage-Empirical Study from Serbia*. 2018. "23 STRATEGIC MANAGEMENT 17".

Central Intelligence Agency (CIA), *Population Comparison - The World Factbook*. https://www.cia.gov/the-world-factbook/field/population/country-comparison/

Commissioner for Information of Public Importance and Personal Data Protection, *The Commissioner Conducts Supervision Procedure in Ministry of Interior, Regarding Suspicion of Facial Recognition Technology Use*. https://tinyurl.com/3ub2bnez

Euronews, *Chinese Police to Help Serbia Cope with Its Workers, Tourists*. https://www.euronews.com/2019/08/02/chinese-police-to-help-serbia-cope-with-its-workers-tourists

European Centre for Press and Media Freedom, *Mapping Media Freedom*. https://www.ecpmf.eu/monitor/mapping-media-freedom/

Freedom House*, Serbia: Freedom on the Net 2024*. https://freedomhouse.org/country/serbia/freedom-net/2024

Serbia: Country Profile. https://freedomhouse.org/country/serbia

D. Golić, *Normative Regulation of Electronic Administration in Republic of Serbia*. 2023. 40 Pravo - teorija i praksa 44. https://orcid.org/0000-0003-2315-5040

G. Gotev, *MEPs Sound the Alarm over Chinese Mass Surveillance Project in Belgrade*. 2021. Euractiv. https://www.euractiv.com/interview/meps-sound-the-alarm-over-chinese-mass-surveillance-project-in-belgrade/

hiljadekamera*, European Promotion of the SHARE Foundation's Book on Biometric Surveillance*. *https://hiljade.kamera.rs/en/*

Huawei Enterprise, *Huawei Safe City Solution: Safeguards Serbia*. https://web.archive.org/web/20190313232443/https://e.huawei.com/en/case-studies/global/2018/201808231012

Industry eLTE Private Network Solution (Huawei Enterprise). https://e.huawei.com/en/solutions/enterprise-wireless/industry-wireless/industrial-elte-private-network> accessed 3 November 2025

J. Jankovic, R. Standish. *Leaked Files Reveal Serbia's Secret Expansion Of Chinese-Made Surveillance*. 2025. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/exclusive-safe-city-china-surveillance-huawei-facial-recognition/33501155.html

N. Jovanovic. *How Serbia Became Blanketed In Chinese-Made Surveillance Cameras*. 2023. Radio Free Europe/Radio Liberty, https://www.rferl.org/a/serbia-surveillance-cameras-china/32526515.html

NN. Kovačević, K. Nenad, A. Mak. *Analysis of the Impact and Actuality of Challenges, Risks and Threats to the Security of the Republic of Serbia*. 2023. 20 Kultura Polisa 146.

D. Krivokapić, *A Disturbing Marriage: Serbia and China Team Up on Digital Surveillance*. 2022. CEPA https://cepa.org/article/a-disturbing-marriage-serbia-and-china-team-up-on-digital-surveillance/

D. Krivokapić, *Starting the Debate on Facial Recognition: A Case Study from Belgrade*'. (Share Foundation 2022).

D. Manojlović, D. Đorđić, V. Jović, *Legal Aspects of Secret Surveillance and Recording and Process Authorities for Its Implemenation: Comparative Research*. 2024. 14 Civitas 188. https://www.ceeol.com/search/article-detail?id=1306100

D. Marković D, CYBERCRIME AND LAW – MANAGING CHALLENGES AND PROSPECTS IN THE DIGITAL AGE. 2025. Pravo - teorija i praksa. https://casopis.pravni-fakultet.edu.rs/index.php/ltp/article/view/898/753

N. Mihaljinac, V. Mevorah, *Broken Promises of Internet and Democracy: Internet Art in Serbia, 1996–2014*. 2019. 41 Media, Culture & Society 889. /doi/pdf/10.1177/0163443719831177?download=true

M. Milošević, *Legal Issues Regarding Secret Communication Surveillance In Serbia*. 2013. 3 International Journal of Economics & Law 118. https://www.ceeol.com/search/article-detail?id=40819

S. Milovanovic, *Application of Internet Technology and Electronic Business Concept in Serbia*. 2015. 19 Procedia Economics and Finance 278. https://www.sciencedirect.com/science/article/pii/S2212567115000283?via%3Dihub

N1 Belgrade, *Thousand Surveillance Cameras in Belgrade – for Safety or Control?*. https://web.archive.org/web/20190517113322/http://rs.n1info.com/English/NEWS/a456797/Belgarde-will-have-1-000-new-survillance-cameras.html

M. Pavlović, *FIGHT AGAINST CYBERCRIME IN SERBIA* - Achievements and Challenges.

B. Popović-Ćitić, S. Djurić, V. Cvetković, *The Prevalence of Cyberbullying among Adolescents: A Case Study of Middle Schools in Serbia*. 2011. 32 School Psychology International 412. /doi/pdf/10.1177/0143034311401700?download=true

Reporters Without Borders (RSF), *World Press Freedom Index 2025*. https://rsf.org/en/index

SHARE Fondacija, N*ew Surveillance Cameras in Belgrade: Location and Human Rights Impact Analysis – "Withheld"*. https://sharefoundation.info/en/new-surveillance-cameras-in-belgrade-location-and-human-rights-impact-analysis-withheld/

DR. Simić, D. Đukanović, S. Mišić, *Sovereignty in Cyberspace: The Case of Serbia Between "Digital Authoritarianism" and "Internet Freedom"*. https://rfpn.fpn.bg.ac.rs/handle/123456789/1444

R. Standish, *Serbia's Legal Tug-Of-War Over Chinese Surveillance Technology (Part 2)*. 2022. Radio Free Europe/Radio Liberty. https://www.rferl.org/a/serbia-chinese-surveilllance-backlash-standish/32145138.html

J. Steele, *What Can We Learn From the Short History of Independent Media in Serbia?* Radio B92, George Soros, and New Models of Media Development. 2024. 29 The International Journal of Press/Politics 646 /doi/pdf/10.1177/19401612231170092?download=true

G. Stojić G, *Internet Usage by the Elderly in Serbia*. 2017. 0 Facta Universitatis, Series: Philosophy, Sociology, Psychology and History 103. https://casopisi.junis.ni.ac.rs/index.php/FUPhilSocPsyHist/article/view/2731

LV. Stošić, AV. Janković, L. Stošić, *CYBERCRIME IN THE REPUBLIC OF SERBIA: PREVALENCE, SITUATION AND PERSPECTIVES*. 2022. 19 KULTURA POLISA 82. https://kpolisa.com/index.php/kp/article/view/1444

Surveillance under Surveillance. https://hiljade.kamera.rs/map/

The Prague Security Studies Institute, *The Sum of All Fears – Chinese AI Surveillance in Serbia*. 2020. https://www.pssi.cz/wp-content/uploads/2025/07/8447_the-sum-of-all-fears-chinese-ai-surveillance-in-serbia.pdf

Tunnard CR, *From State-Controlled Media to the "Anarchy" of the Internet: The Changing Influence of Communications and Information in Serbia in the 1990s*. 2003. 3 Southeast European and Black Sea Studies 97 https://www.tandfonline.com/doi/abs/10.1080/713999348

B. Veljkovic et al., *CYBERBULLYING RESEARCH ON YOUTH POPULATION IN SERBIA*. 2022. 7 RAP CONFERENCE PROCEEDINGS 72

S. Vladisavljev, *How Did Serbia and Huawei Cooperate: A Chronology*. 2019. BFPE. https://en.bfpe.org/in-focus/region-in-focus-focus/how-did-serbia-and-huawei-cooperate-a-chronology/

China's "Digital SilkRoad" Enters theWestern Balkans. (China Observers in Central and Eastern Europe(CHOICE) 2021. https://chinaobservers.eu/wp-content/uploads/2021/06/CHOICE_policy-paper_digital-silk-road_A4_web_04.pdf

V. Vuksanovic, *Securing the Sino-Serbian Partnership*. 2019. Chinaobservers. https://chinaobservers.eu/securing-the-sino-serbian-partnership/

M. Žarković, Z. Ivanović, I. Žarković, *Public Video Surveillance: A Puzzling Issue for Serbian Lawmakers*. 2016. 18 Varstvoslovje: Journal of Criminal Justice & Security 214. https://openurl.ebsco.com/contentitem/gcd:116579650?sid=ebsco:plink:crawler&id=ebsco:gcd:116579650

I. Živković, D. Petrović, *Political (Ab)Use of the Internet- Facebook in Hands of Serbian Right-Wing*. 2024. 66 Sociologija 64. https://doiserbia.nb.rs/Article.aspx?ID=0038-03182401064Z

„dot.pl" - czasopismo Rejestru domeny .pl

Dyrektywa NIS 2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń

Bartosz Głowacki
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0001-6453-2039
E-mail: b.glowacki@awf.katowice.pl

Dominika Grzybowska-Ganszczyk
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0002-6413-306X
E-mail: dominikagrzybowska@yahoo.com

Received: 30.10.2025
Accepted: 09.12.2025
Published: 09.12.2025

Cite this article as:
B. Głowacki, D. Grzybowska-Ganszczyk, *"Dyrektywa NIS 2 jako narzędzie wzmacniania bezpieczeństwa lokalnego i narodowego w obszarze cyberzagrożeń"*

DOT.PL, no. 1/ 2025, 10.60097/DOTPL/215365

Corresponding author:
B. Głowacki, Akademia Wychowania Fizycznego w Katowicach, Polska

E-mail:
b.glowacki@awf.katowice.pl

Streszczenie

Dyrektywa NIS2 oraz nowelizacja polskiej ustawy o krajowym systemie cyberbezpieczeństwa wprowadzają podwyższone wymagania w zakresie zarządzania ryzykiem, raportowania incydentów oraz odpowiedzialności kierowniczej. Artykuł analizuje konsekwencje tych regulacji dla bezpieczeństwa lokalnego i narodowego ze szczególnym uwzględnieniem infrastruktury krytycznej oraz systemów usług kluczowych na poziomie gminnym. W oparciu o analizę aktów prawnych, raportów branżowych oraz literatury naukowej przedstawiono ocenę gotowości organizacyjnej podmiotów zobowiązanych oraz wskazano kluczowe bariery wdrożeniowe. Wyniki wskazują, że efektywność Dyrektywy NIS2 zależy przede wszystkim od zdolności

instytucjonalnych samorządów, skali dostępnych zasobów, a także jakości nadzoru krajowego.

Słowa kluczowe: Dyrektywa NIS2, cyberbezpieczeństwo, bezpieczeństwo lokalne, zarządzanie ryzykiem, infrastruktura krytyczna

NIS 2 Directive as a tool for strengthening local and national security in the area of cyber threats

Abstract

The NIS2 Directive and the amended Polish National Cybersecurity System Act introduce more stringent requirements regarding risk management, incident reporting, and executive accountability. This article examines the implications of these regulations for local and national security, with particular emphasis on critical infrastructure and essential services at the municipal level. Based on an analysis of legal acts, industry reports, and scientific literature, the study evaluates the organizational maturity of obligated entities and identifies key implementation challenges. The findings demonstrate that the effectiveness of Directive NIS2 is highly dependent on institutional capacity, the availability of local resources, and the robustness of national oversight mechanisms.

Keywords: Directive NIS2, cybersecurity, local security, risk management, critical infrastructure

1. Wstęp

Dynamiczna cyfryzacja administracji publicznej, sektora usług oraz infrastruktury krytycznej powoduje znaczący wzrost powierzchni ataku i podatności na incydenty cyberbezpieczeństwa. Raporty i analizy dotyczące cyberzagrożeń w Polsce wskazują na gwałtowny wzrost liczby incydentów w sektorze infrastruktury krytycznej[1]. W ostatnich

[1] Ministerstwo Cyfryzacji. (2025). Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna. Mikrokontroler.pl. . https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-

latach odnotowano istotny wzrost liczby ataków wymierzonych w instytucje publiczne oraz podmioty świadczące usługi społeczne, takie jak wodociągi, transport miejski oraz opieka zdrowotna[2]. Równocześnie raport IBM wskazuje, że średni koszt naruszenia danych w 2023 r. osiągnął najwyższy poziom w historii, co unaocznia skalę problemu i konieczność systemowych działań regulacyjnych. Według raportu IBM Cost of a Data Breach Report 2023 średni globalny koszt naruszenia danych w 2023 roku wyniósł 4,45 mln USD, co stanowi najwyższy poziom w historii tego badania[3].

Odpowiedzią Unii Europejskiej na narastające zagrożenia jest Dyrektywa NIS2, która od 2023 r. ustanawia nowy, bardziej rygorystyczny standard ochrony infrastruktury cyfrowej. Przepisy te rozszerzają katalog podmiotów zobowiązanych i wprowadzają obowiązek wdrożenia zaawansowanych środków zarządzania ryzykiem oraz wzmacniają odpowiedzialność kierownictwa. W Polsce dostosowanie do regulacji unijnych (Dyrektywa NIS2) odbywa się poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC), która wprowadza nowe mechanizmy nadzoru, klasyfikacji podmiotów i reakcji na incydenty[4].

Celem artykułu jest analiza konsekwencji wprowadzenia Dyrektywy NIS2 dla bezpieczeństwa lokalnego i narodowego, ze szczególnym uwzględnieniem uwarunkowań wdrożeniowych po stronie jednostek samorządu terytorialnego. W pracy wykorzystano analizę porównawczą, analizę instytucjonalną oraz przegląd literatury naukowej, raportów branżowych i dokumentów strategicznych.

2. Charakterystyka usług na poziomie lokalnym

Usługi świadczone na poziomie lokalnym stanowią fundament bezpieczeństwa mieszkańców oraz ciągłości funkcjonowania wspólnot samorządowych. Zgodnie z założeniami Dyrektywy NIS2 oraz polskiego systemu krajowego, do usług tych należą

infrastruktura-krytyczna/ (s. 1–2: wzrost liczby incydentów o 60%, w tym ataki na administrację publiczną, transport i ochronę zdrowia).

[2] Cyberataki: trzy atakowane sektory w Polsce - CRN

[3] IBM. (2023). Cost of a Data Breach Report 2023. IBM Report: Half of Breached Organizations Unwilling to Increase https://newsroom.ibm.com/2023-07-24-IBM-Report-H

[4] European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555

m.in. zaopatrzenie w wodę, gospodarka odpadami, transport publiczny, administracja samorządowa, lokalna opieka zdrowotna oraz infrastruktura energetyczna[5]. Są to sektory o szczególnej wrażliwości, których zakłócenie może wywołać szerokie skutki społeczne, ekonomiczne i środowiskowe[6].

Badania ENISA (European Union Agency for Cybersecurity) potwierdzają, że podmioty świadczące publiczne usługi komunalne są szczególnie narażone na cyberataki, ponieważ łączą technologie operacyjne (OT) i systemy informatyczne (IT), które często działają w warunkach ograniczonych zasobów i przestarzałej infrastruktury[7]. W praktyce wiele gmin charakteryzuje się niskim poziomem dojrzałości cyberbezpieczeństwa, w tym brakiem aktualnych procedur reagowania na incydenty oraz niewystarczającym monitoringiem środowiska teleinformatycznego.

Znaczącym wyzwaniem jest również rosnąca zależność administracji samorządowej od usług cyfrowych, w tym systemów klasy ERP, platform komunikacyjnych, systemów rejestru ludności oraz aplikacji umożliwiających obsługę świadczeń społecznych. Jak wskazują badania branżowe, ok. 80% incydentów w sektorze publicznym wynika z błędów ludzkich, niewłaściwego zarządzania dostępem lub phishingu[8]. Pokazuje to, że poza inwestycjami technologicznymi konieczne jest także systemowe wzmacnianie kompetencji pracowników urzędów i jednostek podległych.

Na poziomie lokalnym szczególnego znaczenia nabiera odporność infrastruktury krytycznej o charakterze komunalnym. Wodociągi, oczyszczalnie ścieków, przedsiębiorstwa gospodarki komunalnej oraz operatorzy komunikacji miejskiej stanowią elementy infrastruktury, których unieruchomienie może powodować poważne zagrożenia bezpieczeństwa publicznego.

[5] Biznes.gov.pl. (2024). Walka z cyberprzestępczością – nowe obowiązki firm w dyrektywie NIS2. Warszawa: Ministerstwo Rozwoju i Technologii; s. 2–3
[6] Zuchowska-Prygiel, A. (2025). Implementacja dyrektywy NIS2 w prawie krajowym. Warszawa: Legalis. s. 3–4
[7] European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025 Report. Athens: ENISA; s. 18–20
[8] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 12–14

Incydenty ransomware w amerykańskim Oldsmar (2021)[9] oraz w niemieckich gminach (2023–2025) są często przywoływane jako przykłady podatności systemów OT (Operational Technology) na ataki wymierzone w lokalne zasoby komunalne, takie jak wodociągi i infrastruktura samorządowa[10].

W kontekście Dyrektywy NIS2 podmioty lokalne zostają włączone do szerokiego katalogu operatorów usług kluczowych lub ważnych, co oznacza konieczność dostosowania procesów zarządzania ryzykiem, raportowania incydentów oraz stosowania standardów bezpieczeństwa adekwatnych do poziomu zagrożeń. W praktyce wymaga to głębokiej reorganizacji struktur odpowiedzialnych za cyberbezpieczeństwo, standaryzacji procedur, a także współpracy z podmiotami krajowego systemu reagowania na incydenty.

3. Wymagania NIS2 dla gmin i jednostek im podległych

Dyrektywa NIS2 (Network and Information Security Directive 2), przyjęta w 2022 r., znacząco rozszerza obowiązki w zakresie cyberbezpieczeństwa nakładane na jednostki samorządu terytorialnego (JST). Obejmuje ona zarówno urzędy gmin, jak i podległe im instytucje oraz przedsiębiorstwa komunalne, a jej celem jest podniesienie poziomu bezpieczeństwa cyfrowego usług kluczowych ważnych w całej Unii Europejskiej[11]. W polskim porządku prawnym obowiązki wynikające z Dyrektywy NIS2 wdrażane są poprzez nowelizację ustawy o krajowym systemie cyberbezpieczeństwa (KSC). Nowe przepisy określają szczegółowy zakres wymagań dotyczących zarządzania ryzykiem, raportowania incydentów oraz odpowiedzialności kierowniczej[12].

3.1. Obowiązek wdrożenia środków zarządzania ryzykiem

Dyrektywa NIS2 nakłada na jednostki samorządu terytorialnego (JST) obowiązek wdrożenia kompleksowych środków zarządzania ryzykiem, obejmujących zarówno

[9] Logical Systems Inc. (2021). Security incident at Oldsmar Water Treatment Plant and lessons learned. Oldsmar, FL: Logical Systems Inc; s. 1–2.
[10] The Record. (2023, November 1). Massive ransomware attack hinders services in 70 German municipalities. Recorded Future News; s. 1–2.
[11] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 82–85
[12] Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s.1-3

aspekty techniczne, jak i organizacyjne. Wymagania te obejmują m.in. kontrolę dostępu i uwierzytelnianie wieloskładnikowe, segmentację sieci i ochronę systemów OT, procedury monitorowania i wykrywania incydentów oraz politykę aktualizacji i zarządzania podatnościami na incydenty[13].

Raport Deloitte wskazuje, że dla większości podmiotów publicznych największym wyzwaniem pozostaje brak spójnych metod identyfikacji ryzyk oraz niewystarczająca automatyzacja procesów monitoringu bezpieczeństwa[14]. W przypadku jednostek lokalnych, które często dysponują ograniczonym zapleczem kadrowym i finansowym, wdrożenie wymogów Dyrektyw NIS2 wymaga budowy nowych struktur odpowiedzialnych za cyberbezpieczeństwo lub formalizacji dotychczasowych praktyk ad hoc.

3.2. Obowiązek raportowania incydentów

Dyrektywa NIS 2 wprowadza zawężone ramy czasowe raportowania incydentów o istotnym wpływie na świadczenie usług. Gmina lub jednostka jej podległa zobowiązana jest do: wstępnego zgłoszenia incydentu do CSIRT w ciągu 24 godzin, szczegółowego raportu po 72 godzinach, raportu końcowego po miesiącu od zdarzenia[15].

Z badań ENISA wynika, że krótkie okna raportowania stanowią szczególne wyzwanie dla mniejszych JST, które często nie dysponują zespołami specjalistycznymi pracującymi w trybie całodobowym. W takich przypadkach konieczne staje się korzystanie z usług centrów kompetencyjnych, outsourcingu lub koordynacji międzygminnej.

3.3. Odpowiedzialność kierownicza

Dyrektywa NIS2 wprowadza jeden z najistotniejszych elementów – odpowiedzialność kierowniczą. Oznacza to, że osoby pełniące funkcje zarządcze w jednostkach samorządu terytorialnego (wójt, burmistrz, prezydent miasta, kierownicy jednostek organizacyjnych gmin) ponoszą formalną odpowiedzialność za decyzje dotyczące cyberbezpieczeństwa,

[13] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 95–100

[14] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 14–16

[15] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 101–104

w tym zatwierdzanie polityk i strategii cyberbezpieczeństwa, zapewnienie finansowania środków ochronnych, nadzorowanie wdrożenia rekomendacji pokontrolnych[16].

Ponadto dyrektywa nakłada wymóg szkoleń dla kierownictwa, które mają zapewnić zrozumienie ryzyk oraz odpowiednich mechanizmów zarządzania nimi. Jest to szczególnie istotne na poziomie lokalnym, gdzie decyzje strategiczne podejmowane są często w warunkach ograniczonych kompetencji technicznych.

3.4. Włączenie podmiotów lokalnych do krajowego systemu reagowania

Nowelizacja KSC wprowadza obowiązek ścisłej współpracy podmiotów lokalnych z CSIRT MON, CSIRT NASK i CSIRT GOV. Do europejskiego systemu wymiany informacji o incydentach (EU-CyCLONe) zostają również włączone JST, co ma na celu szybsze reagowanie na zagrożenia transgraniczne[17].

Analizy OECD podkreślają, że skuteczność wdrażania procedur cyberbezpieczeństwa zależy w dużej mierze od zdolności instytucjonalnych najmniejszych gmin. Dla wielu z nich implementacja nowych obowiązków wynikających z Dyrektywy NIS2 i krajowego systemu cyberbezpieczeństwa może wymagać wsparcia zewnętrznego oraz standaryzacji metod wymiany informacji[18].

4. Zarządzanie ryzykiem w jednostkach samorządu terytorialnego (JST)

Dyrektywa NIS2 wskazuje, że zarządzanie ryzykiem cyberbezpieczeństwa jest jednym z kluczowych wymagań dla wszystkich podmiotów świadczących usługi kluczowe i ważne, w tym jednostek samorządu terytorialnego (JST). Wdrożenie tych obowiązków stanowi szczególne wyzwanie dla gmin, które często dysponują ograniczonymi zasobami finansowymi, kadrowymi oraz narzędziowymi[19]. Podmioty objęte regulacją powinny wdrożyć „odpowiednie i proporcjonalne" środki techniczne, operacyjne i organizacyjne

[16] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 105–108

[17] Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s. 3–4

[18] OECD. (2023). Cybersecurity Policy Framework for Local Governments. Paris: Organisation for Economic Co-operation and Development; s. 12–15

[19] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s. 95–100

dostosowane do poziomu ryzyka[20]. W efekcie zarządzanie ryzykiem musi stać się procesem systemowym, ciągłym i udokumentowanym, obejmującym zarówno sferę IT, jak i systemy OT wykorzystywane przez podmioty komunalne (np. wodociągi, oczyszczalnie).

4.1. Identyfikacja i klasyfikacja ryzyk

Proces zarządzania ryzykiem w jednostkach samorządu terytorialnego (JST) powinien rozpoczynać się od identyfikacji zagrożeń w obszarach kluczowych usług lokalnych. W literaturze podkreśla się, że właściwa identyfikacja ryzyk wymaga nie tylko analizy technicznej, lecz także uwzględnienia uwarunkowań organizacyjnych, dostępnych zasobów oraz kontekstu lokalnego[21].

ENISA w swoich raportach podkreśla, że gminy i małe miasta są szczególnie narażone na cyberataki ze względu na dużą liczbę punktów dostępu, brak segmentacji sieci oraz niejednorodność systemów, co zwiększa podatność na zagrożenia[22].

W literaturze oraz raportach dotyczących cyberbezpieczeństwa sektora publicznego podkreśla się, że najczęściej identyfikowane zagrożenia obejmują ataki ransomware wymierzone w urzędy i jednostki komunalne, które prowadzą do paraliżu usług publicznych oraz utraty danych. Istotnym problemem pozostają również próby phishingowe kierowane do pracowników administracyjnych, skutkujące wyłudzeniem danych logowania lub instalacją złośliwego oprogramowania. Kolejną kategorią zagrożeń jest nieautoryzowany dostęp do systemów dokumentacji i rejestrów mieszkańców, co rodzi ryzyko naruszenia poufności danych osobowych. Wskazuje się także na awarie i podatności systemów kadencyjnych oraz finansowych, wynikające z przestarzałej infrastruktury lub błędów w oprogramowaniu, które mogą prowadzić do zakłóceń w funkcjonowaniu instytucji publicznych. Dopełnieniem katalogu zagrożeń są ryzyka

[20] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; art. 21

[21] Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 14–16

[22] European Union Agency for Cybersecurity (ENISA). (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 18–22

fizyczne, takie jak przerwy w dostawie energii, które mogą wpływać na prawidłowe działanie systemów OT (Operational Technology)[23].

Identyfikacja ryzyk powinna obejmować również analizę powiązań pomiędzy systemami informatycznymi gminy a jej jednostkami organizacyjnymi oraz podmiotami zewnętrznymi świadczącymi usługi (np. operatorzy IT, dostawcy Internetu, firmy utrzymaniowe).

4.2. Ocena ryzyka i priorytetyzacja działań

Po identyfikacji zagrożeń konieczna jest ich ocena, która powinna uwzględniać zarówno prawdopodobieństwo wystąpienia incydentu, jak i potencjalne skutki dla świadczenia usług publicznych. Metody oceny ryzyka zalecane przez ENISA obejmują podejścia jakościowe, półilościowe oraz ilościowe, z naciskiem na dostosowanie narzędzi do możliwości instytucji[24].

Dla JST kluczowe jest określenie tzw. „ryzyk krytycznych", czyli tych, których materializacja może doprowadzić do poważnych zakłóceń w działaniu usług komunalnych – np. zatrzymania dostaw wody, unieruchomienia transportu miejskiego lub utraty danych mieszkańców[25]. Wyniki oceny ryzyka powinny stanowić podstawę do opracowania planów zaradczych, polityk bezpieczeństwa oraz planów ciągłości działania (Business Continuity Plan – BCP).

4.3. Wdrażanie środków technicznych i organizacyjnych

Dyrektywa NIS2 w sposób jednoznaczny określa katalog środków technicznych i organizacyjnych, które jednostki samorządu terytorialnego zobowiązane są wdrożyć w ramach skutecznego zarządzania ryzykiem. Wśród najważniejszych zabezpieczeń technicznych wskazuje się wieloskładnikowe uwierzytelnianie, którego celem jest ograniczenie ryzyka przejęcia kont przez osoby nieuprawnione. Istotnym elementem jest również szyfrowanie danych, zapewniające poufność i integralność informacji przetwarzanych w systemach administracyjnych oraz komunalnych. Dyrektywa podkreśla także konieczność stosowania systemów monitorowania logów i wykrywania

[23] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK; s. 40–45
[24] ENISA. (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 20–23
[25] European Union Agency for Cybersecurity (ENISA). (2023). Risk Management Guidelines for the Public Sector. Athens: ENISA; s. 15–18

włamań (IDS/IPS), które umożliwiają bieżące identyfikowanie i reagowanie na incydenty bezpieczeństwa. Ważnym aspektem pozostaje regularne aktualizowanie systemów oraz zarządzanie podatnościami, co pozwala na minimalizację ryzyka wykorzystania luk w oprogramowaniu. Ponadto dokument wskazuje na potrzebę segmentacji sieci oraz ochrony systemów SCADA, co ma szczególne znaczenie w jednostkach komunalnych, gdzie systemy OT, takie jak wodociągi czy transport, muszą być odpowiednio odseparowane od sieci biurowych, aby zapewnić ciągłość działania i odporność na potencjalne zagrożenia[26].

W literaturze naukowej dotyczącej cyberbezpieczeństwa w samorządach lokalnych wskazuje się, że środki organizacyjne obejmują m.in. politykę bezpieczeństwa, szkolenia pracowników, powołanie zespołów ds. cyberbezpieczeństwa, procedury zarządzania dostępem oraz cykliczne audyty bezpieczeństwa[27].

JST muszą także przygotować dokumentację wykazującą zgodność z wymogami Dyrektywy NIS2 – zarówno techniczną, jak i proceduralną. Sama implementacja środków bezpieczeństwa nie jest wystarczająca – konieczne jest także ich udokumentowanie, ponieważ brak dokumentacji może być traktowany jako naruszenie obowiązków zgodności z Dyrektywą NIS2[28].

Dyrektywa NIS2 jednoznacznie wskazuje, że zarządzanie ryzykiem w obszarze cyberbezpieczeństwa nie może być traktowane jako proces jednorazowy, lecz wymaga stałego i systematycznego podejścia. Oznacza to konieczność ciągłego monitorowania zagrożeń oraz bieżącej analizy podatności systemów, aby możliwe było szybkie reagowanie na pojawiające się incydenty. Jednostki samorządu terytorialnego zobowiązane są do przeprowadzania audytów wewnętrznych, które pozwalają ocenić skuteczność wdrożonych procedur i zabezpieczeń, a także audytów zewnętrznych, zapewniających niezależną ocenę zgodności z wymogami Dyrektywy NIS2. Integralnym elementem procesu jest również doskonalenie polityk bezpieczeństwa poprzez

[26]NASK. (2024). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa: Najważniejsze zmiany dla podmiotów. Warszawa: NASK; s. 3–5

[27] Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. *Information, 15*(6), 342. https://doi.org/10.3390/info15060342

[28] Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084; s. 7-8

wdrażanie rekomendacji wynikających z kontroli oraz regularne aktualizowanie stosowanych środków ochronnych. Takie podejście ma na celu nie tylko podniesienie poziomu odporności instytucji publicznych na cyberzagrożenia, lecz także zapewnienie ciągłości działania usług świadczonych obywatelom[29].

Z analiz OECD wynika, że JST najczęściej zaniedbują etap przeglądu ryzyk, co prowadzi do utrzymywania przestarzałych procedur, które nie odpowiadają aktualnym zagrożeniom[30]. W praktyce oznacza to konieczność stałego rozwijania procesów bezpieczeństwa, budowania kompetencji pracowników oraz wzmacniania współpracy z podmiotami wyspecjalizowanymi.

Badania KPMG pokazują, że 68% polskich gmin nie posiada dedykowanego specjalisty ds. cyberbezpieczeństwa, a większość działań realizowana jest przez informatyków pełniących wiele funkcji jednocześnie. To oznacza, że wdrożenie Dyrektywy NIS2 w JST wymaga dodatkowego wsparcia – zarówno w postaci szkoleń, jak i outsourcingu lub współpracy regionalnej[31].

Proofpoint – wskazują, że czynnik ludzki odpowiada za ponad 70% incydentów w sektorze publicznym, co podkreśla konieczność inwestycji w edukację pracowników i budowanie kultury bezpieczeństwa. Dla JST oznacza to, że cyberbezpieczeństwo musi być traktowane strategicznie, jako element zarządzania ryzykiem, a nie tylko obowiązek regulacyjny wynikający z Dyrektywy NIS2[32].

5. Organizacja systemu zarządzania bezpieczeństwem informacji w jednostkach samorządu terytorialnego

Organizacja systemu zarządzania bezpieczeństwem informacji (SZBI) w jednostkach samorządu terytorialnego (JST) jest kluczowa dla osiągnięcia zgodności z Dyrektywą NIS2 oraz zapewnienia cyberodporności usług publicznych. W literaturze

[29] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; s 21–23

[30]OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27-29 https://doi.org/10.1787/9789264987654-en

[31] KPMG. (2024). Barometr cyberbezpieczeństwa 2024: Na fali, czy w labiryncie regulacji? Warszawa: KPMG Polska; s. 27–28

[32] Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10

naukowej podkreśla się, że wdrożenie SZBI zgodnego z normą ISO/IEC 27001 stanowi fundament skutecznej ochrony informacji i zarządzania ryzykiem w sektorze publicznym[33]. Jednostki samorządu terytorialnego (JST) muszą dostosować strukturę systemu zarządzania bezpieczeństwem informacji (SZBI) do własnych możliwości organizacyjnych. Oznacza to uwzględnienie ograniczeń zasobowych, złożoności świadczonych usług oraz specyfiki lokalnej infrastruktury teleinformatycznej. W literaturze naukowej podkreśla się, że wdrożenie SZBI zgodnego z normą ISO/IEC 27001 powinno być elastyczne i proporcjonalne do skali działania instytucji publicznych[34].

5.1. Podstawowe założenia i cele SZBI w JST

Podstawowym celem systemu zarządzania bezpieczeństwem informacji (SZBI) w JST jest zapewnienie integralności, poufności i dostępności informacji przetwarzanych w ramach realizacji zadań publicznych. Norma ISO/IEC 27001 wskazuje, że SZBI powinien być oparty na cyklu PDCA (Plan–Do–Check–Act), który umożliwia ciągłe doskonalenie mechanizmów bezpieczeństwa[35].

W kontekście JST oznacza to konieczność systematycznego planowania i wdrażania polityk, ocen ryzyka, zabezpieczeń oraz mechanizmów kontroli we wszystkich jednostkach podległych urzędowi gminy, powiatu czy województwa.

Dyrektywa NIS2 nakłada na podmioty publiczne – w tym JST – obowiązek wdrożenia „technicznych, operacyjnych i organizacyjnych środków adekwatnych do ryzyka". W praktyce oznacza to konieczność integracji systemu zarządzania bezpieczeństwem informacji (SZBI) z procesem zarządzania usługami publicznymi oraz zarządzania kryzysowego, tak aby cyberbezpieczeństwo było elementem całościowej odporności instytucji[36].

---

[33] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, s. 90–92

[34] Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3),101–118. https://doi.org/10.1016/j.giq.2022.101118; s. 106–107

[35] Peltier, T. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.

[36] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, s. 90–92

Polskie badania NASK wskazują, że JST często wdrażają elementy bezpieczeństwa punktowo, bez spójnego systemu, co prowadzi do braku koordynacji działań oraz nieskuteczności zabezpieczeń[37].

5.2. Struktura organizacyjna SZBI w administracji lokalnej

Efektywne funkcjonowanie SZBI wymaga określenia struktury odpowiedzialności oraz przypisania ról związanych z bezpieczeństwem informacji. W ramach JST podstawowe elementy struktury to: kierownictwo, Inspektor Ochrony Danych (IOD), Zespół ds. Cyberbezpieczeństwa, Administratorzy systemów IT i OT, Kierownictwo.

W literaturze naukowej dotyczącej ISO/IEC 27001 podkreśla się, że najwyższe kierownictwo jednostki ma kluczową rolę w funkcjonowaniu SZBI – musi zapewnić wsparcie dla systemu, zatwierdzać dokumenty polityki bezpieczeństwa oraz gwarantować zasoby niezbędne do ochrony informacji[38]. Badania OECD pokazują, że zaangażowanie najwyższego kierownictwa ma największy wpływ na poziom dojrzałości cyberbezpieczeństwa w sektorze publicznym – bez aktywnego wsparcia liderów instytucji działania w obszarze bezpieczeństwa pozostają fragmentaryczne i nieskuteczne[39].

Inspektor Ochrony Danych (IOD), choć jego podstawowym zadaniem jest nadzór nad zgodnością z RODO, w praktyce odgrywa także istotną rolę w systemie zarządzania bezpieczeństwem informacji (SZBI). Wspiera działania związane z zarządzaniem ryzykiem, uczestniczy w audytach procesów przetwarzania danych oraz doradza w zakresie wdrażania polityk bezpieczeństwa[40].

W literaturze i raportach dotyczących cyberbezpieczeństwa administracji publicznej uwagę zwraca się na fakt iż w wielu jednostkach samorządu terytorialnego (JST) – szczególnie mniejszych – brakuje wyspecjalizowanych zespołów IT. Dlatego praktycznym rozwiązaniem jest tworzenie zespołów międzyjednostkowych lub korzystanie z usług

---

[37] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK.s. 42–44

[38] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), s. 90–92; https://doi.org/10.1108/TQM-09-2020-0202

[39] OECD. (2001). Public Sector Leadership for the 21st Century. Paris: OECD Publishing; s.33–36 https://doi.org/10.1787/9789264195035-en;

[40] Kulesza, J. (2019). Rola inspektora ochrony danych w administracji publicznej. Przegląd Prawa Publicznego, 11(5), s. 28–30

regionalnych centrów kompetencji, które zapewniają wsparcie eksperckie i koordynację działań[41].

5.3.Administratorzy systemów IT i OT

W jednostkach komunalnych (np. wodociągi, transport) administratorzy systemów OT muszą współpracować z IT, co jest szczególnie istotne w świetle rosnącej liczby ataków na infrastrukturę krytyczną[42].

System Zarządzania Bezpieczeństwem Informacji (SZBI) zgodny z ISO/IEC 27001 opiera się na dokumentacji obejmującej m.in.: politykę bezpieczeństwa informacji, politykę zarządzania ryzykiem, instrukcję zarządzania incydentami, politykę klasyfikacji informacji, procedury zarządzania dostępem, rejestry aktywów informacyjnych oraz plany ciągłości działania (BCP) i odtwarzania po awarii (DRP). Literatura naukowa podkreśla, że sukces SZBI zależy od spójności i aktualności dokumentów, a nie tylko od ich formalnego posiadania[43].

W wielu JST dokumenty pozostają nieaktywne lub niekomunikowane pracownikom, co czyni system nieskutecznym. Dyrektywa NIS2 nakłada na podmioty publiczne – w tym JST – obowiązek prowadzenia dokumentacji, która umożliwia wykazanie zgodności podczas kontroli nadzorczych. Brak odpowiednich dowodów (np. polityk, procedur, rejestrów ryzyk, planów ciągłości działania) może być traktowany jako naruszenie obowiązków i skutkować sankcjami administracyjnymi[44].

5.4. Szkolenia i budowanie kultury bezpieczeństwa

Jednym z najsłabszych punktów systemów bezpieczeństwa w administracji publicznej pozostaje czynnik ludzki. Badania Proofpoint wykazują, że ponad 70% incydentów w sektorze publicznym wynika z błędów pracowników lub podatności ludzkich (phishing, błędne decyzje, brak zgłoszeń)[45].

---

[41] NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK;s. 43–45

[42] Wallis, T., & Dorey, P. (2024). Collaboration practices for the cybersecurity of supply chains to critical infrastructure. Applied Sciences, 14(13), 5805. https://doi.org/10.3390/app14135805; s 3–4

[43] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105.; https://doi.org/10.1108/TQM-09-2020-0202; s. 90–92

[44] Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. s. 7–8

[45] Hadlington, L., & Parsons, K. (2017). Human factors in cybersecurity: Examining the role of human error in the public sector. Journal of Information Security and Applications, 34, 41–52. https://doi.org/10.1016/j.jisa.2017.05.002; s. 45-46

Efektywny System Zarządzania Bezpieczeństwem Informacji (SZBI), zgodny z normą ISO/IEC 27001, wymaga wdrożenia działań ukierunkowanych na rozwój kompetencji pracowników oraz budowanie świadomości organizacyjnej w zakresie bezpieczeństwa. Proces ten obejmuje szkolenia wstępne i okresowe dla wszystkich zatrudnionych, które zapewniają podstawową wiedzę o zasadach bezpieczeństwa oraz obowiązkach wynikających z polityk SZBI. Równocześnie konieczne jest prowadzenie specjalistycznych szkoleń dla osób pełniących kluczowe role, takich jak administratorzy systemów IT i OT, członkowie kierownictwa czy inspektorzy ochrony danych, co pozwala na pogłębienie wiedzy technicznej i organizacyjnej. Ważnym elementem systemu są także testy socjotechniczne, w tym symulacje ataków phishingowych, które umożliwiają ocenę podatności pracowników na manipulacje oraz weryfikację skuteczności przeprowadzonych szkoleń. Uzupełnieniem działań edukacyjnych są kampanie uświadamiające dotyczące bezpieczeństwa danych i zasad cyberhigieny, które wspierają budowanie kultury bezpieczeństwa w organizacji i wzmacniają jej odporność na potencjalne incydenty[46].

Budowanie kultury bezpieczeństwa w administracji publicznej powinno być traktowane jako proces ciągły, a nie jednorazowy obowiązek. OECD podkreśla, że organizacje, które wdrożyły model „security by behaviour", osiągają znacząco wyższy poziom cyberodporności, ponieważ bezpieczeństwo staje się elementem codziennych zachowań pracowników, a nie tylko formalną procedurą[47].

5.5. Integracja SZBI z zarządzaniem usługami publicznymi

System Zarządzania Bezpieczeństwem Informacji (SZBI) w jednostkach samorządu terytorialnego nie może funkcjonować w oderwaniu od procesów świadczenia usług publicznych, które w coraz większym stopniu opierają się na wykorzystaniu systemów informatycznych. Skuteczna integracja wymaga powiązania celów bezpieczeństwa z celami strategicznymi JST, tak aby ochrona informacji wspierała realizację misji i usług publicznych, a nie była traktowana jako odrębny obszar działalności. Istotnym

[46] Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003; s. 5-7.
[47] OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD Public Governance Policy Papers, No. 2. Paris: OECD Publishing. https://doi.org/10.1787/f64fed2a-en s.18-20

elementem jest również uwzględnianie wymogów bezpieczeństwa w procedurach zamówień publicznych, co oznacza, że każdy zakup technologii czy usług IT powinien być oceniany pod kątem zgodności z polityką bezpieczeństwa. Równie ważne pozostaje zarządzanie ryzykiem związanym z dostawcami zewnętrznymi, w tym operatorami systemów OT czy dostawcami usług chmurowych, co wymaga stałej kontroli i monitorowania potencjalnych zagrożeń. Ponadto SZBI musi być spójny z planami zarządzania kryzysowego, obejmującymi zarówno ciągłość działania (BCP), jak i odtwarzanie po awarii (DRP), aby zapewnić odporność usług publicznych na zakłócenia i incydenty w obszarze cyberbezpieczeństwa[48].

Dyrektywa NIS2 szczególnie akcentuje odpowiedzialność podmiotów publicznych – w tym JST – za bezpieczeństwo łańcucha dostaw. Oznacza to konieczność monitorowania ryzyka związanego z wykonawcami usług IT oraz operatorami infrastruktury krytycznej. Brak nadzoru nad dostawcami był jedną z głównych przyczyn incydentów w europejskich gminach w latach 2020–2023, co potwierdzają raporty ENISA i OECD[49].

6. Reagowanie na incydenty i zarządzanie ciągłością działania w JST

Dyrektywa NIS2 jednoznacznie podkreśla, że reagowanie na incydenty cyberbezpieczeństwa stanowi jeden z podstawowych obowiązków jednostek samorządu terytorialnego. Regulacja nakłada na podmioty publiczne konieczność opracowania procedur obejmujących detekcję, analizę, obsługę oraz raportowanie incydentów, tak aby zapewnić spójny i skuteczny proces reagowania. Wymaga również wdrożenia systemów gwarantujących ciągłość działania usług kluczowych, co ma szczególne znaczenie w kontekście świadczenia usług publicznych o krytycznym znaczeniu dla obywateli. Dyrektywa wskazuje ponadto na obowiązek terminowego zgłaszania incydentów do właściwych organów nadzorczych, co umożliwia koordynację działań i zwiększa efektywność odpowiedzi na zagrożenia. Integralną częścią procesu jest także powiązanie planów reagowania z planami zarządzania kryzysowego oraz planami ciągłości działania

[48] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96. s. 91–93

[49] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152; art. 21–23

(BCP/DRP), co pozwala na zapewnienie odporności instytucji publicznych na zakłócenia i szybkie przywrócenie funkcjonowania usług po wystąpieniu incydentu[50].

Reagowanie na incydenty powinno być traktowane jako integralny element Systemu Zarządzania Bezpieczeństwem Informacji (SZBI), a nie jako odrębny proces uruchamiany wyłącznie w sytuacjach zagrożenia. Oznacza to, że procedury detekcji, analizy, obsługi i raportowania incydentów muszą być wpisane w codzienne funkcjonowanie organizacji, powiązane z politykami bezpieczeństwa, zarządzaniem ryzykiem oraz planami ciągłości działania[51].

6.1. Rodzaje incydentów cyberbezpieczeństwa w JST

JST są narażone na różnorodne rodzaje incydentów, w tym ataki ransomware, naruszenia danych osobowych, zakłócenia w systemach usług komunalnych, kompromitację kont pracowników czy ataki DDoS na serwisy internetowe[52].

Analizy ENISA wskazują, że sektor publiczny w Europie stał się jednym z głównych celów grup cyberprzestępczych, szczególnie ze względu na stosunkowo niski poziom zabezpieczeń oraz wysoką wartość danych przetwarzanych przez administrację lokalną[53].

W gminach szczególnie istotne są incydenty wpływające na systemy OT (Operational Technology), takie jak wodociągi, stacje uzdatniania wody czy sieci ciepłownicze. Ataki na te elementy mogą prowadzić do poważnych konsekwencji dla bezpieczeństwa mieszkańców[54].

6.2. Proces reagowania na incydenty

Proces reagowania na incydenty cyberbezpieczeństwa, zgodnie z dobrymi praktykami rekomendowanymi przez NIST oraz ENISA, powinien obejmować pięć kluczowych etapów. Pierwszym z nich jest przygotowanie, które polega na opracowaniu

---

[50] ENISA. (2023). Incident Response in the Public Sector: Guidelines for NIS2 Implementation. Athens: European Union Agency for Cybersecurity; s. 12–16

[51] Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105.; https://doi.org/10.1108/TQM-09-2020-0202; s. 91–92

[52] NASK. Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023; Warszawa, s. 42–45

[53] ENISA. Threat Landscape 2023. Athens: European Union Agency for Cybersecurity. s. 22–25

[54] Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96; s. 92–94

planów reagowania, przeprowadzeniu szkoleń dla zespołów odpowiedzialnych za bezpieczeństwo, wdrożeniu narzędzi detekcji oraz precyzyjnym zdefiniowaniu ról i obowiązków. Kolejnym etapem jest identyfikacja, obejmująca wykrywanie anomalii, analizę alertów oraz ustalenie, czy dane zdarzenie rzeczywiście stanowi incydent wymagający reakcji. Następnie następuje ograniczenie skutków, czyli szybkie działania minimalizujące skalę zniszczeń, takie jak odseparowanie zainfekowanej sieci, blokowanie kont czy zamykanie podatnych usług. Czwarty etap to eliminacja i odzyskiwanie, który dotyczy przywracania systemów do pełnej sprawności poprzez usuwanie złośliwego oprogramowania, odtwarzanie danych z kopii zapasowych oraz weryfikację poprawności działania systemów po incydencie. Ostatnim elementem procesu są działania po incydencie, obejmujące analizę przyczyn zdarzenia, sporządzenie raportu końcowego oraz aktualizację procedur i zabezpieczeń w celu zwiększenia odporności organizacji na przyszłe zagrożenia[55].

Dyrektywa NIS2 nakazuje prowadzenie dokumentacji operacji wykonywanych na każdym etapie obsługi incydentu, co ma kluczowe znaczenie przy audytach oraz ewentualnym postępowaniu administracyjnym[56].

6.3. Raportowanie incydentów zgodnie z Dyrektywą NIS2

Dyrektywa NIS2 precyzyjnie określa wieloetapowy system raportowania incydentów cyberbezpieczeństwa, który ma na celu zapewnienie szybkiej reakcji oraz skutecznej koordynacji działań pomiędzy podmiotami publicznymi a właściwymi organami nadzorczymi. Proces ten rozpoczyna się od wstępnego zgłoszenia incydentu do odpowiedniego CSIRT, które musi zostać dokonane w ciągu 24 godzin od jego wykrycia. Następnie, w terminie do 72 godzin, wymagane jest przekazanie szczegółowego raportu incydentu, obejmującego opis zdarzenia, jego przebieg oraz podjęte działania zaradcze. Ostatnim etapem jest sporządzenie raportu końcowego, zawierającego analizę przyczyn incydentu, ocenę zastosowanych środków oraz wskazanie ryzyka dalszej eskalacji. Tak

[55] Alhassan, I., Sammon, D., & Daly, M. (2020). Critical success factors for incident response capability in public sector organizations. Government Information Quarterly, 37(4), 101–112. https://doi.org/10.1016/j.giq.2020.101112; s. 105–107

[56] European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. art. 23–28

zdefiniowany system raportowania ma na celu nie tylko zwiększenie przejrzystości i szybkości reakcji, lecz także budowanie odporności instytucji publicznych na przyszłe zagrożenia[57].

Badania EY i ENISA wskazują, że w europejskich gminach najczęstszą przeszkodą w terminowym raportowaniu jest brak procedur wewnętrznych określających przepływ informacji i odpowiedzialności.

6.4. Planowanie ciągłości działania (BCP) i odtwarzanie po awarii (DRP)

Zarządzanie ciągłością działania stanowi kluczowy element budowania odporności jednostek samorządu terytorialnego na incydenty związane z cyberbezpieczeństwem. Zgodnie z wymaganiami normy ISO 22301 organizacje zobowiązane są do opracowania planu BCP, który obejmuje kompleksową analizę wpływu incydentów na działalność (Business Impact Analysis – BIA), pozwalającą na ocenę potencjalnych skutków zakłóceń dla realizacji usług publicznych. Istotnym etapem jest identyfikacja procesów krytycznych, których utrzymanie ma zasadnicze znaczenie dla funkcjonowania instytucji, oraz określenie zasobów niezbędnych do ich nieprzerwanej realizacji. Plan powinien również zawierać procedury alternatywne, umożliwiające świadczenie usług w sposób zastępczy, na przykład poprzez ręczne wykonywanie wybranych czynności administracyjnych. Integralną częścią systemu jest zapewnienie kopii zapasowych oraz redundancji danych, co pozwala na szybkie odtworzenie zasobów informacyjnych i minimalizację skutków potencjalnych incydentów[58].

Plan DRP (Disaster Recovery Plan) dotyczy technicznych aspektów odtwarzania systemów IT i OT po incydencie, szczególnie po ataku ransomware lub awarii infrastruktury.

W praktyce wiele JST posiada jedynie szczątkowe plany ciągłości działania lub ogranicza je do formalnych zapisów, które nie zostały przetestowane w warunkach rzeczywistych.

6.5. Ćwiczenia i testowanie procedur

[57] Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3), 101–118. https://doi.org/10.1016/j.giq.2022.101118 s. 106–107

[58] ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva: International Organization for Standardization. s. 12–18

Normy ISO 27001 oraz ISO 22301 jednoznacznie wskazują na konieczność cyklicznego testowania mechanizmów bezpieczeństwa i ciągłości działania, co stanowi kluczowy element budowania odporności organizacyjnej. Wymóg ten obejmuje regularne sprawdzanie procedur reagowania na incydenty, weryfikację skuteczności działań zespołów odpowiedzialnych za bezpieczeństwo, kontrolę poprawności kopii zapasowych oraz testowanie planów BCP i DRP. Praktyka administracji publicznej pokazuje, że instytucje, które systematycznie przeprowadzają ćwiczenia i symulacje, znacząco skracają czas reakcji na incydenty oraz redukują koszty związane z ich obsługą. Wyniki badań Gartnera potwierdzają, że brak testów planów odtwarzania stanowi jeden z głównych czynników zwiększających skalę i skutki incydentów w jednostkach sektora publicznego, co podkreśla wagę regularnej weryfikacji i doskonalenia procedur bezpieczeństwa[59].

6.6. Współpraca z CSIRT i partnerami zewnętrznymi

Jednostki samorządu terytorialnego, zgodnie z wymaganiami Dyrektywy NIS2, zobowiązane są do utrzymywania stałego kontaktu z właściwymi podmiotami odpowiedzialnymi za bezpieczeństwo cybernetyczne oraz zapewnienie ciągłości działania usług publicznych. Oznacza to konieczność współpracy z CSIRT MON, CSIRT GOV oraz CSIRT NASK, które pełnią rolę krajowych zespołów reagowania na incydenty i wspierają procesy detekcji, analizy oraz obsługi zdarzeń.

Równocześnie JST muszą pozostawać w bieżącej komunikacji z dostawcami usług IT i operatorami łączności, aby zapewnić skuteczne zarządzanie ryzykiem wynikającym z korzystania z infrastruktury teleinformatycznej.

Integralnym elementem systemu współpracy jest także kontakt z jednostkami komunalnymi, takimi jak wodociągi czy transport publiczny, które odpowiadają za funkcjonowanie systemów OT i stanowią kluczowe ogniwo w zapewnieniu bezpieczeństwa oraz odporności lokalnych usług krytycznych[60].

[59]Gartner. (2021). Best Practices for Business Continuity and Disaster Recovery Testing. Stamford: Gartner Research. s. 7–9

[60] NASK. Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. s. 40–43; Warszawa: NASK.

W literaturze wskazuje się, że współpraca międzyinstytucjonalna jest kluczowa dla skutecznego reagowania na incydenty. Modele „security ecosystem" zwiększają wymianę informacji, podnoszą świadomość zagrożeń i umożliwiają szybszą neutralizację ataków[61].

Podsumowanie

Wprowadzenie Dyrektywy NIS2 stanowi punkt zwrotny w podejściu państw członkowskich Unii Europejskiej do kwestii cyberbezpieczeństwa, w szczególności w sektorze publicznym. Jednostki samorządu terytorialnego (JST), odpowiedzialne za realizację kluczowych usług publicznych, stają przed koniecznością wdrożenia mechanizmów ochronnych o znacznie wyższym poziomie dojrzałości niż dotychczas. Analiza przeprowadzona w pracy potwierdza, że Dyrektywa NIS2 nie jest wyłącznie aktem prawnym narzucającym nowe obowiązki, lecz przede wszystkim narzędziem wzmacniającym odporność cyfrową lokalnych wspólnot poprzez wymóg systemowego podejścia do bezpieczeństwa informacji.

Wskazano, że cyberzagrożenia dla JST są zróżnicowane, rosną dynamicznie i obejmują zarówno ataki na klasyczne systemy IT, jak i na infrastrukturę OT wykorzystywaną przez jednostki komunalne. Równocześnie analiza obowiązków wynikających z Dyrektywy NIS2 – takich jak zarządzanie ryzykiem, raportowanie incydentów czy nadzór nad łańcuchem dostaw – dowodzi, że gminy, powiaty i województwa muszą opracować spójne systemy organizacyjne i proceduralne, aby móc spełnić wymagania regulacyjne.

Podkreślono kluczowe znaczenie budowy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI) jako podstawy wdrożenia Dyrektywy NIS2. SZBI łączy elementy organizacyjne, techniczne i edukacyjne, umożliwiając standaryzację działań oraz ciągłe doskonalenie procesów bezpieczeństwa. Jego integralnymi komponentami są: polityki bezpieczeństwa, analiza ryzyka, klasyfikacja informacji, nadzór nad usługodawcami, plan ciągłości działania oraz procedury reagowania na incydenty.

[61] Bada, A., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for a security ecosystem. Information & Computer Security, 27(2), 224–242. https://doi.org/10.1108/ICS-04-2018-0042; s. 230–233

Przeprowadzona analiza wykazała jednocześnie, że głównymi barierami wdrażania Dyrektywy NIS2 w JST są: ograniczenia kadrowe, niedostateczny poziom specjalizacji pracowników, brak centralizacji zarządzania, niewystarczające finansowanie oraz niska świadomość zagrożeń. Wskazuje to na konieczność rozwijania współpracy między jednostkami samorządowymi, tworzenia centrów kompetencji, a także wdrażania programów szkoleniowych ukierunkowanych na podniesienie kultury bezpieczeństwa w administracji lokalnej.

Szczególne znaczenie ma również zarządzanie incydentami i ciągłością działania, które – zgodnie z wymogami Dyrektywy NIS2 – powinny stanowić procesy stałe, regularnie testowane i dostosowywane do zmieniającego się krajobrazu zagrożeń. JST muszą więc nie tylko reagować na incydenty, lecz także rozwijać zdolności proaktywne: monitorować infrastrukturę, analizować podatności, prowadzić ćwiczenia i audyty, utrzymywać kontakt z CSIRT oraz instytucjami nadzorczymi. Dyrektywa NIS2 powinna być postrzegana nie jako obciążenie administracyjne, lecz jako szansa na trwałe podniesienie poziomu bezpieczeństwa cyfrowego oraz profesjonalizację zarządzania usługami publicznymi. Efektywne wdrożenie Dyrektywy NIS2 wymaga jednak działań wielowymiarowych: wsparcia kierownictwa, rozwijania kompetencji, inwestycji w technologie, przejrzystych procedur oraz współpracy międzyinstytucjonalnej.

Wnioskiem końcowym jest stwierdzenie, że implementacja Dyrektywy NIS2 w polskich JST może stać się impulsem do budowy nowoczesnego, odpornego ekosystemu administracji lokalnej, opartego na zarządzaniu ryzykiem, profesjonalizacji procesów i podejściu „cybersecurity by design". Warunkiem powodzenia jest jednak odejście od działań incydentalnych na rzecz trwałej, systemowej transformacji sposobu organizacji bezpieczeństwa informacji.

Bibliografia

1. Alhassan, I., Sammon, D., & Daly, M. (2020). Critical success factors for incident response capability in public sector organizations. Government Information Quarterly, 37(4), 101–112. https://doi.org/10.1016/j.giq.2020.101112; s. 105–107.
2. Alshaikh, M. (2020). Developing cybersecurity culture to influence employee behavior: A practice perspective. Computers & Security, 98, 102003. https://doi.org/10.1016/j.cose.2020.102003; s. 5–7.
3. Bada, A., & Nurse, J. R. C. (2019). Developing cybersecurity education and awareness programmes for a security ecosystem. Information & Computer Security, 27(2), 224–242. https://doi.org/10.1108/ICS-04-2018-0042; s. 230–233.

4. Biznes.gov.pl. . (2024). Walka z cyberprzestępczością – nowe obowiązki firm w dyrektywie NIS2. Warszawa: Ministerstwo Rozwoju i Technologii; s. 2–3.
5. CRN. (2025). Cyberataki: trzy atakowane sektory w Polsce.
6. Culot, G., Nassimbeni, G., Podrecca, M., & Sartor, M. (2021). The ISO/IEC 27001 information security management standard: Literature review and theory-based research agenda. The TQM Journal, 33(7), 76–105. https://doi.org/10.1108/TQM-09-2020-0202; s. 90–92, 91–92.
7. Deloitte. (2024). Cyberbezpieczeństwo w administracji publicznej: Wyzwania i rekomendacje. Warszawa: Deloitte Polska; s. 12–14. — tamże, s. 14–16.
8. ENISA. (2023). Incident Response in the Public Sector: Guidelines for NIS2 Implementation. Athens: European Union Agency for Cybersecurity; s. 12–16.
9. ENISA. (2023). Threat Landscape 2023. Athens: European Union Agency for Cybersecurity; s. 22–25.
10. ENISA. (2024). ENISA Threat Landscape 2024. Athens: ENISA; s. 18–22, 20–23.
11. European Union. (2022). Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 — tamże, s. 82–85. — tamże, s. 95–100. — tamże, s. 101–104. — tamże, s. 105–108. — tamże, art. 21, art. 21–23, art. 23–28.
12. European Union Agency for Cybersecurity (ENISA). (2023). Risk Management Guidelines for the Public Sector. Athens: ENISA; s. 15–18.
13. European Union Agency for Cybersecurity (ENISA). (2025). ENISA Threat Landscape 2025 Report. Athens: ENISA; s. 18–20.
14. Gartner. (2021). Best Practices for Business Continuity and Disaster Recovery Testing. Stamford: Gartner Research; s. 7–9.
15. Hadlington, L., & Parsons, K. (2017). Human factors in cybersecurity: Examining the role of human error in the public sector. Journal of Information Security and Applications, 34, 41–52. https://doi.org/10.1016/j.jisa.2017.05.002; s. 45–46.
16. Hossain, S. T., Yigitcanlar, T., Nguyen, K., & Xu, Y. (2024). Understanding local government cybersecurity policy: A concept map and framework. Information, 15(6), 342. https://doi.org/10.3390/info15060342..
17. IBM. (2023). Cost of a Data Breach Report 2023. IBM Report: Half of Breached Organizations Unwilling to Increase. https://newsroom.ibm.com/2023-07-24-IBM-Report-H
18. ISO. (2019). ISO 22301:2019 Security and resilience – Business continuity management systems – Requirements. Geneva: International Organization for Standardization; s. 12–18.
19. Kankanhalli, A., & Lim, J. (2022). Building cyber resilience in public sector organizations: The role of ISO/IEC 27001. Government Information Quarterly, 39(3), 101–118. https://doi.org/10.1016/j.giq.2022.101118; s. 106–107.
20. KPMG. (2024). Barometr cyberbezpieczeństwa 2024: Na fali, czy w labiryncie regulacji? Warszawa: KPMG Polska; s. 27–28.
21. Kozakiewicz, A., & Nowak, J. (2023). Zarządzanie bezpieczeństwem informacji w administracji publicznej w kontekście dyrektywy NIS2. Zeszyty Naukowe Politechniki Śląskiej. Organizacja i Zarządzanie, 167, 85–96; s. 90–92, 91–93, 92–94.
22. Kulesza, J. (2019). Rola inspektora ochrony danych w administracji publicznej. Przegląd Prawa Publicznego, 11(5), s. 28–30.
23. Logical Systems Inc. (2021). Security incident at Oldsmar Water Treatment Plant and lessons learned. Oldsmar, FL: Logical Systems Inc; s. 1–2.
24. Ministerstwo Cyfryzacji. (2024). Projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa – implementacja dyrektywy NIS2. Warszawa: Gov.pl.; s. 1–3. — tamże, s. 3–4.
25. Ministerstwo Cyfryzacji. (2025). Cyberzagrożenia w Polsce 2025: Najczęściej atakowana infrastruktura krytyczna. Mikrokontroler.pl. . https://mikrokontroler.pl/2025/04/25/cyberzagrozenia-w-polsce-2025-najczesciej-atakowana-infrastruktura-krytyczna/ (s. 1–2: wzrost liczby incydentów o 60%, w tym ataki na administrację publiczną, transport i ochronę zdrowia).
26. NASK. (2024). Raport o stanie bezpieczeństwa cyberprzestrzeni RP 2023. Warszawa: NASK; s. 40–45, 42–44, 43–45.
27. NASK. (2024). Nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa: Najważniejsze zmiany dla podmiotów. Warszawa: NASK; s. 3–5.

28. OECD. (2001). Public Sector Leadership for the 21st Century. Paris: OECD Publishing; s. 33–36. https://doi.org/10.1787/9789264195035-en..
29. OECD. (2020). The OECD Digital Government Policy Framework: Six dimensions of a Digital Government. OECD Public Governance Policy Papers, No. 2. Paris: OECD Publishing. https://doi.org/10.1787/f64fed2a-en; s. 18–20.
30. OECD. (2023). Cybersecurity Policy Framework for Local Governments. Paris: Organisation for Economic Co-operation and Development; s. 12–15.
31. OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27–29. https://doi.org/10.1787/9789264987654-en..
32. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.
33. Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10.
34. OECD. (2023). Digital resilience in local public services. Paris: OECD Publishing; s. 27–29. https://doi.org/10.1787/9789264987654-en..
35. Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. Boca Raton: Auerbach Publications; s. 45–47.
36. Proofpoint. (2023). Human Factor Report 2023. Sunnyvale, CA: Proofpoint Inc; s. 8–10.
37. Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084; s. 7–8.
38. Wallis, T., & Dorey, P. (2024). Collaboration practices for the cybersecurity of supply chains to critical infrastructure. Applied Sciences, 14(13), 5805. https://doi.org/10.3390/app14135805; s. 3–4.

„dot.pl" - czasopismo Rejestru domeny .pl

Cyberbezpieczeństwo w cyberprzestrzeni. Zagrożenia i aspekty ochrony w dobie sztucznej inteligencji.

Dominika Grzybowska-Ganszczyk
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0002-6413-306X
E-mail: dominikagrzybowska@yahoo.com
Bartosz Głowacki
Akademia Wychowania Fizycznego w Katowicach, Polska
ORCID: https://orcid.org/0000-0001-6453-2039
E-mail: b.glowacki@awf.katowice.pl
Janusz Mikitin
Uczelnia Nauk Społecznych, Polska
ORCID: https://orcid.org/0009-0006-6908-7193
E-mail: J.miki@wp.pl

Received: 30.10.2025
Accepted: 09.12.2025
Published: 09.12.2025

Cite this article as:
D. Grzybowska-Ganszczyk, B. Głowacki, J. Mikitin, "*Cyberbezpieczeństwo w cyberprzestrzeni. Zagrożenia i aspekty ochrony w dobie sztucznej inteligencji*"

DOT.PL, no. 1/ 2025, 10.60097/DOTPL/215385

Corresponding author:
Dominika Grzybowska-Ganszczyk, Akademia Wychowania Fizycznego w Katowicach, Polska

E-mail: dominikagrzybowska@yahoo.com

Streszczenie

Postęp technologiczny XXI wieku przyniósł ludzkości ogromne możliwości w zakresie komunikacji, pracy, nauki oraz rozwoju społeczno-gospodarczego. Jednocześnie dynamiczny rozwój technologii cyfrowych doprowadził do pojawienia się nowych, coraz bardziej złożonych zagrożeń, które w istotny sposób wpływają na poczucie bezpieczeństwa jednostki oraz funkcjonowanie całych państw. Cyberprzestrzeń stała się jednym z kluczowych obszarów aktywności człowieka, co potwierdzają najnowsze raporty ENISA i IBM Security. Jedną z podstawowych potrzeb człowieka, według piramidy Abrahama Maslowa, jest potrzeba bezpieczeństwa –

obecnie jednak jest ona coraz częściej naruszana w wyniku incydentów mających miejsce w cyberprzestrzeni.
Celem niniejszej pracy jest analiza zjawiska cyberzagrożeń oraz ich wpływu na bezpieczeństwo jednostkowe i zbiorowe. Artykuł przedstawia definicje i charakterystykę cyberprzestrzeni, omawia główne rodzaje zagrożeń cyfrowych, w tym zagrożenia rozwijające się wraz z postępem sztucznej inteligencji. W pracy zaprezentowano także aspekty prawne i instytucjonalne cyberbezpieczeństwa w Polsce i Unii Europejskiej, wskazując najważniejsze dokumenty, wśród których kluczową rolę odgrywa Dyrektywa NIS2. Rozwinięto także analizę roli czynnika ludzkiego, wskazując, iż – jak podkreśla raport Verizon – większość incydentów wynika z błędów użytkowników. W końcowej części omówiono przykłady incydentów cyberprzestępczych w Polsce oraz zaprezentowano rekomendacje wzmacniające odporność cyfrową społeczeństwa.
Opracowanie ma charakter analityczno-opisowy i podkreśla, że rozwój technologii, mimo licznych korzyści, niesie ze sobą także rosnące ryzyko utraty danych, prywatności i zaufania społecznego. Świadomość zagrożeń oraz edukacja w zakresie cyberbezpieczeństwa stanowią istotne składowe zapewnienia stabilności i bezpieczeństwa w świecie cyfrowym.

Słowa kluczowe: : cyberbezpieczeństwo, cyberprzestrzeń, cyberzagrożenia, phishing, ransomware

Cybersecurity in cyberspace. Threats and protection aspects in the age of artificial intelligence.

Abstract
The technological progress of the twenty-first century has brought humanity immense opportunities in communication, work, education, and socio-economic development. At the same time, the dynamic growth of digital technologies has led to the emergence of new, increasingly complex threats that significantly affect both individual perceptions of security and the

functioning of entire states. Cyberspace has become one of the key domains of human activity, as confirmed by recent reports from ENISA and IBM Security. According to Abraham Maslow's hierarchy of needs, security is one of the fundamental human requirements; however, it is increasingly compromised by incidents occurring in cyberspace. The aim of this study is to analyze the phenomenon of cyber threats and their impact on individual and collective security. The article presents definitions and characteristics of cyberspace, discusses the main categories of digital threats—including those evolving alongside advances in artificial intelligence—and examines the legal and institutional aspects of cybersecurity in Poland and the European Union, highlighting key documents such as the NIS2 Directive. The analysis also addresses the human factor, emphasizing—as noted in the Verizon report—that most incidents stem from user errors. The final section discusses examples of cybercrime incidents in Poland and provides recommendations for strengthening the digital resilience of society.

This study adopts an analytical-descriptive approach and underscores that technological development, despite its numerous benefits, also entails growing risks of data loss, privacy breaches, and erosion of public trust. Awareness of threats and education in the field of cybersecurity are essential components for ensuring stability and security in the digital world.

Keywords: cybersecurity, cyberspace, cyber threats, phishing, ransomware

Wstęp

Rozwój technologii informacyjno-komunikacyjnych znacząco zmienił sposób funkcjonowania współczesnych społeczeństw. W literaturze anglojęzycznej podkreśla się, że cyberprzestrzeń stała się „kolejną domeną prowadzenia konfliktów”[1], a aktywność cyberprzestępcza wzrosła zarówno w skali, jak i w poziomie skomplikowania.

[1] M.D., Cavelty, T. Pulver, M., *Smeets, Ewolucja studiów nad cyberkonfliktami*, “International Affairs”, tom 100, numer 6, 2024, s. 2317–2339, https://doi.org/10.1093/ia/iiae175

Według raportu Microsoft Security z 2023 roku odnotowano wyraźny wzrost aktywności grup przestępczych oraz kampanii socjotechnicznych[2].

Postęp technologiczny w XXI wieku przyniósł liczne innowacje, które znacząco ułatwiają codzienne życie. Rozwój narzędzi teleinformatycznych umożliwia szybką komunikację, handel elektroniczny, zdalną edukację oraz efektywną administrację publiczną. Jednocześnie niesie ze sobą liczne zagrożenia, które mogą naruszać podstawowe potrzeby człowieka, w tym potrzebę bezpieczeństwa wskazywaną w piramidzie Maslowa. Cyberprzestrzeń daje ogromne możliwości rozwoju, ale każde zdarzenie o charakterze przestępczym w tej sferze może na trwałe zakłócić poczucie bezpieczeństwa użytkowników[3].

Zmiana sposobu korzystania z narzędzi cyfrowych była szczególnie widoczna w okresie pandemii COVID-19. Wówczas wiele zajęć edukacyjnych zostało przeniesionych na platformy e-learningowe i komunikatory grupowe, takie jak Microsoft Teams czy Zoom. Zakupy, które wcześniej odbywały się w tradycyjnych sklepach, przeniosły się na platformy internetowe, np. Allegro czy Zalando. Również administracja publiczna musiała szybko dostosować swoje funkcjonowanie do nowego środowiska cyfrowego, co zwiększyło ryzyko cyberzagrożeń. W tym czasie pojawiły się m.in. . złośliwe oprogramowania zawierające w nazwie słowa „COVID" lub „corona", wzrosła liczba oszustw internetowych i ataków phishingowych, a także intensyfikowały się działania szkodliwego oprogramowania skierowane przeciwko infrastrukturze krytycznej, np. szpitalom[4]. Analiza cyberbezpieczeństwa wymaga zrozumienia cyberprzestrzeni jako pojęcia oraz mechanizmów jej funkcjonowania. Chociaż cyberprzestrzeń nie posiada jednej spójnej definicji, literatura przedmiotu oraz dokumenty strategiczne – np. Doktryna cyberbezpieczeństwa RP – podkreślają znaczenie bezpieczeństwa w przestrzeni cyfrowej, wymieniając jej główne elementy: ochronę strategicznych zasobów państwa,

[2]Microsoft Digital Defense Report 2023. Redmond: Microsoft Security. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

[3]Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs). Information and Computer Security, tom 27, nr 3, s. 393–410, https://doi.org/10.1108/ICS-07-2018-0080

[4]Kaspersky. (2021). COVID-19 and Cybersecurity Threats: Global Report. Moscow: Kaspersky Lab. Kaspersky Security Bulletin 2021 – Securelist; https://securelist.com/ksb-2021/

bezpieczeństwo przetwarzania informacji, funkcjonowanie sieci teleinformatycznych, ochronę informacji niejawnych i prawo do prywatności[5].

Bezpieczeństwo w cyberprzestrzeni jest kluczowe nie tylko dla państw i instytucji, ale również dla pojedynczych użytkowników, gdyż cyberzagrożenia stają się coraz bardziej złożone i trudne do przewidzenia. Dlatego istotne jest zarówno zrozumienie natury zagrożeń, jak i wdrażanie odpowiednich działań prewencyjnych, które pozwolą chronić informacje oraz infrastrukturę krytyczną w cyfrowym świecie[6].

Cyberprzestrzeń – charakterystyka i znaczenie

Wielu badaczy zwraca uwagę, że cyberprzestrzeń jest środowiskiem dynamicznym, pozbawionym granic fizycznych i podatnym na zakłócenia[7]. Obejmuje ona infrastrukturę teleinformatyczną, dane, usługi cyfrowe oraz relacje zachodzące pomiędzy użytkownikami. Doktryna Cyberbezpieczeństwa RP definiuje cyberprzestrzeń jako „przestrzeń przetwarzania informacji tworzona przez systemy teleinformatyczne i użytkowników". W literaturze i raportach podkreśla się, że ochrona infrastruktury krytycznej nabiera coraz większego znaczenia, ponieważ stała się jednym z głównych celów ataków ransomware – szczególnie w sektorach energii, transportu i ochrony zdrowia[8]. Analizę zagadnienia cyberprzestrzeni warto rozpocząć od samej definicji, co pozwoli na dalsze rozważania dotyczące bezpieczeństwa cyfrowego. Pojęcie cyberprzestrzeni rozwinęło się dzięki cybernetyce, jednak jego znaczenie i zakres ewoluowały w ciągu ostatnich kilkudziesięciu lat.

W literaturze przedmiotu często przywołuje się Williama Gibsona, autora powieści Burning Chrome, który określił cyberprzestrzeń jako „królestwo przestrzennych paradoksów". Od czasu wydania książki minęło ponad 30 lat, jednak wizja przedstawiona

[5] M. Carr, Public–private partnerships in national cyber-security strategies. International Affairs, 2016, 92(1),ss. 43–62, https://doi.org/10.1111/1468-2346.12504

[6] ENISA. (2023). ENISA Threat Landscape 2023. Athens: European Union Agency for Cybersecurity

[7] M. Foulon, G. Meibauer, *How cyberspace affects international relations: The promise of structural modifiers*. "Contemporary Security Policy", 2024, 45(3), ss. 426–458, https://doi.org/10.1080/13523260.2024.2365062

[8] Dragos Industrial Ransomware Analysis: Q4 2024 https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024

w powieści znalazła odzwierciedlenie w rzeczywistości – cyberprzestrzeń stała się integralną częścią życia codziennego[9].

Nie istnieje jedna, spójna definicja cyberprzestrzeni. Pojęcie to jest używane zarówno przez organizacje rządowe, polityków, jak i specjalistów ds. bezpieczeństwa. Najczęściej odnosi się do opisu zagrożeń w sieci oraz sposobów przeciwdziałania im. Przykłady definicji przedstawiają Paulina Tekielska i Łukasz Czekaj: „Cyberprzestrzeń to sieć powiązań między jednostkami sprzętowymi i centralnymi, umożliwiająca przesyłanie informacji oraz zapewniająca przestrzeń i środki do ich przetwarzania[10].”

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024, zastąpiła wcześniejsze ramy polityki i doktrynę Cyberbezpieczeństwa RP z 2015 roku. Strategia ta podkreśla, że cyberprzestrzeń to środowisko przetwarzania i wymiany informacji, tworzone przez systemy teleinformatyczne, użytkowników oraz relacje między nimi, a jej ochrona obejmuje zarówno sektor publiczny, prywatny, jak i wojskowy[11]. Z powyższych definicji wynika, że cyberprzestrzeń charakteryzuje się następującymi cechami: jest przestrzenią nieograniczoną, funkcjonuje dzięki sieciom teleinformatycznym oraz służy wymianie informacji. Bezpieczeństwo w cyberprzestrzeni stanowi wielowymiarowy obszar badań i praktyki, obejmujący zarówno aspekty technologiczne, jak i prawne oraz organizacyjne. Istotne komponenty tego bezpieczeństwa to ochrona strategicznych zasobów państwa, zapewnienie dokładności i wiarygodności przetwarzanych informacji, utrzymanie sprawnego funkcjonowania sieci teleinformatycznych oraz infrastruktury krytycznej, a także ochrona informacji niejawnych i ustawowo chronionych przy jednoczesnym poszanowaniu prawa do prywatności[12].

W literaturze podkreśla się, że cyberprzestrzeń jest środowiskiem szczególnie podatnym na zakłócenia, a jej ochrona wymaga zintegrowanego podejścia łączącego technologie, regulacje i edukację społeczną. Pomimo stosowania zaawansowanych systemów

---

[9] T.R., Andersen, (2019). *Cyberspace Revisited: A Radial Reading of William Gibson's "Burning Chrome".* "Journal of American Culture", vol. 42(2), ss. 121–136, https://doi.org/10.1111/jacc.13019

[10] B. Farrand, H. Carrapico, A. Turobov, *Nowa geopolityka cyberbezpieczeństwa UE: bezpieczeństwo, gospodarka i suwerenność*, „International Affairs", tom 100, numer 6, 2024, ss. 2379–2397, https://doi.org/10.1093/ia/iiae231

[11] Digital Skills and Jobs Platform. (2023). Poland – Cybersecurity Strategy of the Republic of Poland 2019–2024. Updated March 27, 2023. Retrieved from Digital Skills & Jobs EU

[12] B. Farrand, H. Carrapico, A. Turobov, (2024). *The new geopolitics of EU cybersecurity: security, economy and sovereignty.* „International Affairs", vol. 100(6), ss. 2379–2397. https://doi.org/10.1093/ia/iiae231

monitoringu i detekcji, pełne określenie wszystkich danych dotyczących cyberataków pozostaje trudne ze względu na anonimowość sprawców, transnarodowy charakter działań oraz złożoność incydentów, które często obejmują wiele warstw infrastruktury cyfrowej i wymagają współpracy międzynarodowej w zakresie ich przeciwdziałania (Farrand, Carrapico, & Turobov, 2024).

Cyberbezpieczeństwo można postrzegać jako system porządkujący struktury cyberprzestrzeni, którego celem jest zapewnienie stabilności i odporności środowiska cyfrowego. Do jego głównych zadań należy ochrona poufności informacji, zabezpieczenie danych i prywatności użytkowników, a także ochrona infrastruktury krytycznej przed zagrożeniami, w tym cyberterroryzmem. Istotnym elementem jest również utrzymanie ciągłości i sprawności zasobów niezbędnych do świadczenia e-usług, które stały się fundamentem funkcjonowania administracji publicznej, gospodarki oraz życia społecznego. W literaturze podkreśla się, że cyberbezpieczeństwo nie jest jedynie zbiorem technicznych procedur, lecz systemem integrującym aspekty prawne, organizacyjne i edukacyjne, co pozwala na skuteczniejsze przeciwdziałanie zagrożeniom i budowanie odporności instytucji oraz obywateli[13].

Cyberprzestrzeń jest dynamicznym środowiskiem, w którym rozwój technologii niesie zarówno ogromne możliwości, jak i nowe zagrożenia, wymagające odpowiednich działań ochronnych oraz prewencyjnych.

Klasyczne cyberzagrożenia

Phishing pozostaje najpowszechniejszą formą ataku cybernetycznego. Według danych ENISA ponad 80% incydentów inicjowanych jest poprzez manipulację socjotechniczną[14]. Podobną tendencję obserwuje Microsoft, wskazując na rosnący poziom profesjonalizacji kampanii phishingowych. Ransomware stał się natomiast najbardziej kosztownym

[13] E. Claessen, (2020). *Przekształcanie Internetu – wpływ sekurytyzacji infrastruktury internetowej na podejścia do zarządzania Internetem: przypadek Rosji i UE*. „Journal of Cyber Policy", vol. 5(1), ss.140–157. https://doi.org/10.1080/23738871.2020.1728356

[14]ENISA Threat Landscape 2024 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

rodzajem ataku – IBM X-Force wskazuje, że średni koszt incydentu w 2023 roku przekroczył 1,5 mln USD[15].

1. **Charakterystyka cyberzagrożeń**

Cyberzagrożenia są konsekwencją rosnącej roli technologii w życiu codziennym oraz funkcjonowaniu państw i organizacji. Ich głównymi celami mogą być: kradzież środków pieniężnych, zakłócenie pracy firm, szpiegostwo i nielegalne pozyskiwanie informacji. Każda informacja w świecie cyfrowym podlega różnym zagrożeniom. Incydent bezpieczeństwa to zdarzenie zagrażające poufności, integralności lub dostępności danych. W kontekście ochrony informacji kluczowe jest stosowanie działań prewencyjnych, ponieważ lepiej zapobiegać niż naprawiać skutki ataku.

2. **Najczęściej występujące cyberzagrożenia**

Cyberzagrożenia przybierają różnorodne formy i obejmują zarówno klasyczne, jak i coraz bardziej zaawansowane techniki ataków. Do najczęściej spotykanych należą złośliwe oprogramowanie (malware), którego celem jest uszkodzenie urządzenia lub przejęcie informacji, a także phishing – polegający na wyłudzaniu danych poprzez fałszywe wiadomości e-mail lub strony internetowe. Szczególnie niebezpieczną odmianą jest spear phishing, w którym atakujący podszywa się pod osobę znaną ofierze. Istotnym zagrożeniem pozostaje również atak typu Man-in-the-Middle (MitM), polegający na przechwyceniu komunikacji między dwiema stronami. Do kategorii szkodliwego oprogramowania zaliczają się m.in. . konie trojańskie, które podszywają się pod legalne aplikacje w celu infekowania systemu, oraz ransomware, szyfrujące dane ofiary i żądające okupu za ich odblokowanie. Wśród poważnych incydentów bezpieczeństwa wymienia się także ataki typu Denial of Service (DoS/DDoS), polegające na przejęciu funkcji wielu urządzeń w celu zakłócenia działania systemu docelowego[16].

Coraz częściej zagrożenia dotyczą urządzeń Internetu Rzeczy (IoT), takich jak kamery czy czujniki, które często działają na przestarzałym oprogramowaniu. Do typowych incydentów zalicza się także wycieki danych – obejmujące kradzież informacji

[15]Microsoft. (2024). Microsoft Digital Defense Report 2024. Security Insider. Retrieved December 7, 2025, from https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024; ss. 27-66.

[16] Por. J. R. Vacca (red.), Computer and Information Security Handbook, 3rd Edition, Elsevier, 2017; ss.215

osobowych, finansowych lub poufnych – oraz złośliwe aplikacje mobilne, instalowane w celu uzyskania dostępu do wrażliwych danych użytkownika.

Dodatkowo raporty wskazują na inne formy zagrożeń między innymi: zagrożenia wewnętrzne wynikające z działań pracowników, ingerencje fizyczne, uszkodzenia lub kradzieże systemów, kradzież kryptowalut[17].

3. Współczesne tendencje

Wraz z rozwojem technologii rośnie liczba potencjalnych celów cyberataków, a grupy przestępcze coraz bardziej specjalizują się w ich planowaniu. Coraz częściej obserwuje się współpracę pomiędzy organizacjami cyberprzestępczymi oraz udostępnianie narzędzi w formie „gotowych komponentów", co umożliwia osobom o ograniczonym doświadczeniu prowadzenie działalności cyberprzestępczej[18].

Zagrożenia związane ze sztuczną inteligencją

Rozwój sztucznej inteligencji (AI) otworzył nowe możliwości w zakresie automatyzacji procesów, analizy danych oraz wspierania decyzji strategicznych. Jednocześnie jednak pojawiły się nowe formy zagrożeń, które znacząco komplikują krajobraz cyberbezpieczeństwa. Nowoczesne modele sztucznej inteligencji umożliwiają generowanie niezwykle przekonujących treści, takich jak deepfake, które – jak wskazuje Europol – znacząco zwiększają skuteczność oszustw finansowych. Technologia ta wykorzystywana jest nie tylko do manipulacji wizerunkiem osób publicznych, lecz także w atakach socjotechnicznych, gdzie fałszywe nagrania audio lub wideo służą do wyłudzania danych bądź środków finansowych[19].

Szczególnie groźnym zjawiskiem w obszarze sztucznej inteligencji jest adversarial machine learning, czyli manipulowanie danymi treningowymi lub wejściowymi modeli w celu uzyskania błędnych wyników. Ataki tego typu mogą prowadzić do kompromitacji systemów bezpieczeństwa – przykładowo poprzez błędną klasyfikację obrazów w

[17] J. R. Vacca, (Ed.). (2017). Computer and information security handbook (3rd ed.). Elsevier; s. 233.

[18] H. S. Lallie, L. A. Shepherd, J. R. C. Nurse, A. Erola, G. Epiphaniou, C. Maple, X. Bellekens, X. (2021). *Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic*. "Computers & Security", vol. 105, ss.2-4. https://doi.org/10.1016/j.cose.2021.102248;

[19] Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol Innovation Lab. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes; ss. 14-20.

systemach monitoringu czy generowanie fałszywych alarmów w systemach wykrywania intruzów[20].

Wraz z rozwojem technologii sztucznej inteligencji pojawiają się nowe formy zagrożeń, w tym ataki wspierane przez AI, które stają się coraz bardziej autonomiczne i trudniejsze do wykrycia. Modele te mogą adaptować swoje strategie w czasie rzeczywistym, co znacząco utrudnia ich neutralizację przez tradycyjne systemy bezpieczeństwa[21].

Do największych zagrożeń związanych ze sztuczną inteligencją zalicza się manipulację obrazem, dźwiękiem i tekstem w postaci deepfake oraz innych treści generatywnych, które mogą być wykorzystywane do oszustw finansowych, dezinformacji czy szantażu. Istotnym problemem pozostaje również adversarial machine learning, polegający na celowym wprowadzaniu błędów do danych treningowych lub wejściowych, co prowadzi do kompromitacji modeli. Coraz większe znaczenie mają także autonomiczne ataki AI-powered, w których systemy uczą się samodzielnie i adaptują swoje strategie, przez co stają się trudniejsze do wykrycia przez klasyczne narzędzia bezpieczeństwa. Wreszcie, sztuczna inteligencja znajduje zastosowanie w cyberprzestępczości zorganizowanej, gdzie algorytmy wspierają automatyzację phishingu, ransomware czy ataków DDoS[22].

Aspekty prawne i instytucjonalne

Cyberbezpieczeństwo w Europie i Polsce opiera się na rozbudowanych regulacjach prawnych oraz strukturach instytucjonalnych, które mają na celu zwiększenie odporności państw i organizacji na rosnące zagrożenia cyfrowe.

Najważniejszym dokumentem regulującym kwestie bezpieczeństwa w Unii Europejskiej jest Dyrektywa NIS2, której celem jest zwiększenie odporności sektorów kluczowych i ważnych[23].

---

[20]B. Biggio, F. Roli, (2018). *Wild patterns: Ten years after the rise of adversarial machine learning*.“Pattern Recognition”, vol. 84, ss. 317–331. https://doi.org/10.1016/j.patcog.2018.07.023

[21] L. Huang, A. D. Joseph, B. Nelson, B. I. P. Rubinstein, J. D. Tygar, (2020). *Adversarial machine learning: A survey of attacks on machine learning systems*. “ACM Computing Surveys”, vol. *53*(3), ss. 1–43.

[22]M. Brundage, S. Avin, J. Clark, H. Toner, P. Eckersley, B. Garfinkel, B. et al.,(2018*). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint arXiv:1802.07228; s.12

[23] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. “International Cybersecurity Law Review”, vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4; s.210

Dyrektywę NIS2 uzupełnia Cybersecurity Act, który ustanawia europejski system certyfikacji bezpieczeństwa, wzmacniając zaufanie do usług cyfrowych i produktów ICT. W Polsce kluczowe znaczenie ma natomiast ustawa o krajowym systemie cyberbezpieczeństwa, która precyzuje zadania CSIRT GOV, CSIRT MON oraz CSIRT NASK, zapewniając koordynację działań w zakresie reagowania na incydenty i podnoszenia odporności infrastruktury krytycznej[24].

1. **Regulacje unijne**

Regulacje unijne w obszarze cyberbezpieczeństwa obejmują szereg kluczowych dokumentów. Dyrektywa NIS (UE 2016/1148) nakłada na państwa członkowskie obowiązki dotyczące bezpieczeństwa sieci i systemów informatycznych, wymagając m.in. . opracowania krajowej strategii bezpieczeństwa, powołania zespołów reagujących na incydenty (CSIRT) oraz ustalenia zasad zgłaszania incydentów przez operatorów usług kluczowych i cyfrowych. Strategia Cyberbezpieczeństwa UE, aktualizowana w latach 2017, 2020 i 2023, koncentruje się na odporności, prewencji i ochronie, umożliwia korzystanie z wiarygodnych komponentów cyfrowych oraz wzmacnia zdolność państw członkowskich do przeciwdziałania cyberzagrożeniom. Uzupełnieniem tych działań jest Cybersecurity Act (2019), który wprowadza europejski system certyfikacji bezpieczeństwa, mający na celu podniesienie zaufania do usług cyfrowych i produktów ICT[25].

2. **Regulacje krajowe – Polska**

W Polsce podstawowym aktem prawnym regulującym kwestie bezpieczeństwa cyfrowego jest ustawa z 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, która określa ramy prawne i instytucjonalne dla działań związanych z ochroną cyberprzestrzeni. Dokument ten wskazuje m.in. . na funkcjonowanie trzech zespołów CSIRT: CSIRT GOV, któremu przewodniczy szef Agencji Bezpieczeństwa Wewnętrznego;

[24]European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, ss. 15–69. http://data.europa.eu/eli/reg/2019/881/oj;

[25] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. "International Cybersecurity Law Review", vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4

CSIRT MON, przyporządkowany Ministrowi Obrony Narodowej; oraz CSIRT NASK, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy. Rozwiązania te mają na celu zapewnienie skutecznej koordynacji działań w zakresie reagowania na incydenty i podnoszenia odporności krajowej infrastruktury krytycznej[26].

Obowiązki operatorów infrastruktury kluczowej obejmują m.in.: szacowanie ryzyka, wdrażanie środków technicznych, gromadzenie informacji o podatności systemu, prowadzenie działań związanych z incydentami oraz zapewnienie skutecznej komunikacji w przypadku zagrożeń[27].

Najbardziej zaawansowane systemy ochrony danych mogą okazać się nieskuteczne, jeśli użytkownicy nie przestrzegają podstawowych zasad bezpieczeństwa lub stają się ofiarami manipulacji psychologicznej. Do najczęstszych przyczyn udanych cyberataków należą korzystanie z prostych lub powtarzalnych haseł, brak aktualizacji urządzeń i oprogramowania, ignorowanie zasad ograniczonego zaufania wobec wiadomości e-mail czy linków oraz nieświadome udostępnianie danych osobowych w mediach społecznościowych. Z kolei zasady ograniczające ryzyko obejmują stosowanie silnych i unikalnych haseł wraz z weryfikacją dwuetapową, regularne aktualizacje systemów i aplikacji, używanie programów antywirusowych i narzędzi szyfrujących, zachowanie ograniczonej ufności w kontaktach online, weryfikację podejrzanych wiadomości oraz ochronę prywatności w mediach społecznościowych i komunikatorach[28].

Wnioski i podsumowanie

Cyberbezpieczeństwo stanowi obecnie jeden z najważniejszych filarów funkcjonowania państwa i społeczeństwa informacyjnego. Współczesne zagrożenia – od klasycznych form ataków, takich jak phishing czy ransomware, po nowoczesne wyzwania

[26] A. Klimkiewicz, (2020). Krajowy system cyberbezpieczeństwa – założenia i praktyka. Przegląd Prawa i Administracji, vol. 121, ss. 83–96. Wrocław: Uniwersytet Wrocławski. https://doi.org/10.19195/0137-1134.121.6

[27] F. Teichmann, (2025). *Cybersecurity of critical infrastructure in Europe: the NIS2 directive in focus*. "International Cybersecurity Law Review", vol. 6(2), ss. 207–220. https://doi.org/10.1365/s43439-025-00154-4

[28] M. Abidin, A. Nawawi, A. Salin, (2019), *Bezpieczeństwo danych klientów i kradzież: doświadczenie malezyjskiej organizacji.* „Information and Computer Security", tom 27 nr 1, ss. 81–100, https://doi.org/10.1108/ICS-04-2018-0043

związane ze sztuczną inteligencją – pokazują, że bezpieczeństwo cyfrowe jest procesem dynamicznym i wielowymiarowym. Wymaga ono nie tylko stosowania zaawansowanych technologii ochronnych, lecz także odpowiednich regulacji prawnych oraz szeroko zakrojonej edukacji społecznej[29]. Rozwój sztucznej inteligencji tworzy zarówno nowe szanse, jak i ryzyka. Z jednej strony umożliwia skuteczniejsze wykrywanie incydentów oraz automatyzację działań obronnych, z drugiej – generuje nowe typy zagrożeń, takie jak deepfake czy adversarial machine learning. Technologie te mogą być wykorzystywane zarówno w celu poprawy bezpieczeństwa, jak i w działaniach przestępczych, co czyni cyberprzestrzeń obszarem szczególnie podatnym na dynamiczne i trudne do przewidzenia wyzwania[30]. W literaturze podkreśla się, że systemy sztucznej inteligencji mogą znacząco zwiększać odporność organizacji poprzez wspieranie procesów wykrywania incydentów i automatyzację działań obronnych. Jednocześnie wskazuje się, iż wymagają one odpowiednich ram prawnych i etycznych, które ograniczałyby ryzyko nadużyć oraz zapewniały zgodność z zasadami odpowiedzialnego wykorzystania technologii[31].

Regulacje prawne, takie jak Dyrektywa NIS2 oraz Cybersecurity Act, stanowią fundament dla budowania odporności instytucji publicznych i prywatnych w Europie. Dokumenty te rozszerzają zakres obowiązków w zakresie cyberbezpieczeństwa, obejmując nowe sektory i podmioty, a także wprowadzają europejski system certyfikacji bezpieczeństwa, który ma na celu podniesienie zaufania do usług cyfrowych i produktów ICT. W literaturze podkreśla się, że regulacje te są kluczowe dla zapewnienia wysokiego poziomu ochrony infrastruktury krytycznej oraz dla harmonizacji działań państw członkowskich[32].

Wdrażanie regulacji dotyczących cyberbezpieczeństwa w państwach członkowskich, w tym w Polsce, pokazuje, że skuteczna ochrona cyberprzestrzeni wymaga współpracy

---

[29] A. Piazza, S. Vasudevan, M. Carr, *Cyberbezpieczeństwo na uniwersytetach w Wielkiej Brytanii: mapowanie (lub zarządzanie) udostępnianiem informacji wywiadowczych o zagrożeniach w sektorze szkolnictwa wyższego*,"Journal of Cybersecurity", tom 9, numer 1, 2023, tyad019, s. 214; https://doi.org/10.1093/cybsec/tyad019

[30] M. Brundage et al., (2018). *The malicious use of artificial intelligence: Forecasting, prevention, and mitigation*. arXiv preprint arXiv:1802.07228. https://arxiv.org/abs/1802.07228

[31] L. Floridi et al., (2018). *AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations*. "Minds and Machines", vol. 28(4), ss. 689–707. https://doi.org/10.1007/s11023-018-9482-5

[32] J. Ruohonen, (2024). *A systematic literature review on the NIS2 Directive*. arXiv preprint arXiv:2412.08084. s.6 https://arxiv.org/abs/2412.08084

międzyinstytucjonalnej oraz integracji działań na poziomie lokalnym, narodowym i europejskim. Tylko skoordynowane podejście, obejmujące zarówno instytucje publiczne, jak i prywatne, pozwala na budowanie odporności wobec rosnącej liczby zagrożeń cyfrowych oraz zapewnia harmonizację standardów bezpieczeństwa w całej Europie[33]. Nie można jednak zapominać o czynniku ludzkim. Najbardziej zaawansowane systemy ochrony danych mogą okazać się nieskuteczne, jeśli użytkownicy nie stosują podstawowych zasad bezpieczeństwa lub stają się ofiarami manipulacji psychologicznej. W literaturze podkreśla się, że to właśnie zachowania i nawyki użytkowników – takie jak korzystanie ze słabych haseł, brak ostrożności wobec wiadomości e-mail czy podatność na socjotechnikę – stanowią jeden z głównych czynników ryzyka w obszarze cyberbezpieczeństwa[34].

Podsumowując, cyberbezpieczeństwo należy traktować jako proces ciągły, wymagający integracji działań prawnych, technologicznych i edukacyjnych. Tylko w ten sposób możliwe jest zapewnienie odporności państw, instytucji i obywateli na rosnące zagrożenia w cyberprzestrzeni. Jak wskazują Kasper i Vernygora (2021), Unia Europejska stopniowo buduje swoją strategiczną narrację w obszarze cyberbezpieczeństwa, łącząc elementy odporności, odstraszania i współpracy międzynarodowej. W tym kontekście edukacja społeczna oraz podnoszenie świadomości użytkowników stają się równie istotne jak regulacje prawne i innowacyjne technologie, ponieważ dopiero ich wspólne zastosowanie pozwala na skuteczne wzmacnianie odporności cyfrowej w dynamicznie zmieniającym się środowisku globalnym[35].

Bibliografia

1. Abidin, M. A. Z., Nawawi, A., & Salin, A. S. A. P. (2019). Bezpieczeństwo danych klientów i kradzież: doświadczenie malezyjskiej organizacji. Information & Computer Security, 27(1), 81–100. https://doi.org/10.1108/ICS-04-2018-0043
2. Andersen, T. R. (2019). Cyberspace revisited: A radial reading of William Gibson's "Burning Chrome". Journal of American Culture, 42(2), 121–136. https://doi.org/10.1111/jacc.13019

[33] M. Carr, (2021). *The EU's cybersecurity strategy: A framework for resilience*. "Journal of Cyber Policy", vol. 6(1), ss. 1–20. https://doi.org/10.1080/23738871.2021.1884802

[34] L. Hadlington, (2017). *Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours*. "Heliyon", vol. 3(7), e00346, ss. 489–497. https://doi.org/10.1016/j.heliyon.2017.e00346

[35] A. Kasper, V. A. Vernygora, (2021). *Cybersecurity of the EU: A strategic narrative of a cyber power or a confusing policy for a local common market?* "Cuadernos Europeos de Deusto", vol. 65(2021), ss. 29–71 https://doi.org/10.18543/ced-65-2021pp

3. Biggio, B., & Roli, F. (2018). Wild patterns: Ten years after the rise of adversarial machine learning. Pattern Recognition, 84, 317–331. https://doi.org/10.1016/j.patcog.2018.07.023
4. Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., ... & Amodei, D. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. arXiv preprint arXiv:1802.07228. https://arxiv.org/abs/1802.07228
5. Carr, M. (2016). Public–private partnerships in national cyber-security strategies. International Affairs, 92(1), 43–62. https://doi.org/10.1111/1468-2346.12504
6. Carr, M. (2021). The EU's cybersecurity strategy: A framework for resilience. Journal of Cyber Policy, 6(1), 1–20. https://doi.org/10.1080/23738871.2021.1884802
7. Claessen, E. (2020). Przekształcanie internetu – wpływ sekurytyzacji infrastruktury internetowej na podejścia do zarządzania internetem: przypadek Rosji i UE. Journal of Cyber Policy, 5(1), 140–157. https://doi.org/10.1080/23738871.2020.1728356
8. Digital Skills and Jobs Platform. (2023). Poland – Cybersecurity Strategy of the Republic of Poland 2019–2024. Updated March 27, 2023. Retrieved from Digital Skills & Jobs EU.
9. Dragos. (2024). Industrial Ransomware Analysis: Q4 2024. Retrieved from https://www.dragos.com/blog/dragos-industrial-ransomware-analysis-q4-2024
10. Dunn Cavelty, M., Pulver, T., & Smeets, M. (2024). The evolution of cyber conflict studies. International Affairs, 100(6), 2317–2339. https://doi.org/10.1093/ia/iiae175
11. ENISA. (2023). ENISA Threat Landscape 2023. Athens: European Union Agency for Cybersecurity.
12. ENISA. (2024). ENISA Threat Landscape 2024. Athens: European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024
13. European Parliament & Council of the European Union. (2019). Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69. http://data.europa.eu/eli/reg/2019/881/oj
14. Europol. (2022). Facing reality? Law enforcement and the challenge of deepfakes. Europol Innovation Lab. https://www.europol.europa.eu/publications-events/publications/facing-reality-law-enforcement-and-challenge-of-deepfakes
15. Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. International Affairs, 100(6), 2379–2397. https://doi.org/10.1093/ia/iiae231
16. Floridi, L., Cowls, J., Beltrametti, M., Chatila, R., Chazerand, P., Dignum, V., ... & Vayena, E. (2018). AI4People—An ethical framework for a good AI society: Opportunities, risks, principles, and recommendations. Minds and Machines, 28(4), 689–707. https://doi.org/10.1007/s11023-018-9482-5
17. Foulon, M., & Meibauer, G. (2024). How cyberspace affects international relations: The promise of structural modifiers. Contemporary Security Policy, 45(3), 426–458. https://doi.org/10.1080/13523260.2024.2365062
18. Hadlington, L. (2017). Human factors in cybersecurity; examining the link between Internet addiction, impulsivity, attitudes towards cybersecurity, and risky cybersecurity behaviours. Heliyon, 3(7), e00346, 489–497. https://doi.org/10.1016/j.heliyon.2017.e00346
19. Huang, L., Joseph, A. D., Nelson, B., Rubinstein, B. I. P., & Tygar, J. D. (2020). Adversarial machine learning: A survey of attacks on machine learning systems. ACM Computing Surveys, 53(3), 1–43.
20. Kasper, A., & Vernygora, V. A. (2021). Cybersecurity of the EU: A strategic narrative of a cyber power or a confusing policy for a local common market? Cuadernos Europeos de Deusto, 65(2021), 29–71. https://doi.org/10.18543/ced-65-2021pp
21. Kaspersky. (2021). COVID-19 and Cybersecurity Threats: Global Report. Moscow: Kaspersky Lab. Kaspersky Security Bulletin 2021 – Securelist. https://securelist.com/ksb-2021/
22. Klimkiewicz, A. (2020). Krajowy system cyberbezpieczeństwa – założenia i praktyka. Przegląd Prawa i Administracji, 121, 83–96. Wrocław: Uniwersytet Wrocławski. https://doi.org/10.19195/0137-1134.121.6
23. Lallie, H. S., Shepherd, L. A., Nurse, J. R. C., Erola, A., Epiphaniou, G., Maple, C., & Bellekens, X. (2021). Cyber security in the age of COVID-19: A timeline and analysis of cyber-crime and cyber-attacks during the pandemic. Computers & Security, 105, 102248. https://doi.org/10.1016/j.cose.2021.102248
24. Microsoft. (2023). Microsoft Digital Defense Report 2023. Redmond: Microsoft Security. https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report

25. Microsoft. (2024). Microsoft Digital Defense Report 2024. Security Insider. Retrieved December 7, 2025, from https://www.microsoft.com/en-us/security/security-insider/threat-landscape/microsoft-digital-defense-report-2024
26. Piazza, A., Vasudevan, S., & Carr, M. (2023). Cybersecurity in UK universities: Mapping (or managing) threat intelligence sharing within the higher education sector. Journal of Cybersecurity, 9(1), tyad019. https://doi.org/10.1093/cybsec/tyad019
27. Ruohonen, J. (2024). A systematic literature review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. https://arxiv.org/abs/2412.08084
28. Teichmann, F. (2025). Cybersecurity of critical infrastructure in Europe: The NIS2 directive in focus. International Cybersecurity Law Review, 6(2), 207–220. https://doi.org/10.1365/s43439-025-00154-4
29. Vacca, J. R. (Ed.). (2017). Computer and information security handbook (3rd ed.). Elsevier.

„dot.pl" - czasopismo Rejestru domeny .pl

Piractwo w sieci w kontekście utworów muzycznych - współczesne zagrożenia i konsekwencje prawne

Elżbieta Skrzek
Akademia Leona Koźmińskiego, Warszawa, Polska
ORCID: https://orcid.org/0009-0007-8463-3137
E-mail: ella.skrzek@gmail.com

Streszczenie

Artykuł analizuje zjawisko piractwa muzycznego w sieci, ze szczególnym uwzględnieniem jego współczesnych form oraz konsekwencji prawnych wynikających z naruszenia praw autorskich do utworów muzycznych. W pierwszej części omówiono pojęcie piractwa w sieci oraz aktualną skalę zjawiska. Przedstawiono również współczesne formy piractwa muzycznego w sieci, obejmujące *peer-to-peer*, *stream-ripping*, nielegalne serwisy internetowe, wykorzystywanie fragmentów utworów w mediach społecznościowych, a także wykorzystywanie muzyki poprzez systemy sztucznej inteligencji. W dalszej części pracy przeanalizowano odpowiedzialność cywilną i karną użytkowników oraz platform internetowych. Następnie omówiono konsekwencje piractwa dla twórców oraz przedstawiono metody przeciwdziałania piractwu wskazując na potrzebę kompleksowego podejścia łączącego instrumenty prawne, technologiczne i edukacyjne. Artykuł podkreśla,

Received: 03.12.2025
Accepted: 18.12.2025
Published: 18.12.2025

Cite this article as:
E. Skrzek, "*Piractwo w sieci w kontekście utworów muzycznych - współczesne zagrożenia i konsekwencje prawne*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/215788

Corresponding author:
Elżbieta Skrzek, Akademia Leona Koźmińskiego, Warszawa, Polska

E-mail: ella.skrzek@gmail.com

że skuteczna ochrona muzyki w środowisku cyfrowym wymaga współpracy twórców, platform internetowych oraz ustawodawcy, a także dostosowania istniejących regulacji do dynamicznie zmieniającej się rzeczywistości technologicznej.

Słowa kluczowe: piractwo muzyczne; utwory muzyczne; prawo autorskie; naruszenia online; streaming

Piracy in the online environment in the context of musical works - contemporary threats and legal consequences

Abstract

The article examines the phenomenon of online music piracy, with particular emphasis on its contemporary forms and the legal consequences arising from the infringement of copyrights in musical works. The first part discusses the notion of online piracy and the current scale of the phenomenon. It further presents modern forms of online music piracy, including peer-to-peer sharing, stream-ripping, illegal online services, the use of music fragments on social media, as well as the exploitation of musical content by artificial intelligence systems. The subsequent sections analyse the civil and criminal liability of users and online platforms. The article then addresses the consequences of piracy for creators and outlines methods of combating it, highlighting the need for a comprehensive approach combining legal, technological and educational measures. It ultimately argues that the effective protection of music in the digital environment requires cooperation between creators, online platforms and legislators, as well as the adaptation of existing regulations to a rapidly evolving technological landscape.

Keywords: music piracy, musical works, copyright law, online infringements, streaming

1. Wprowadzenie

Dynamiczny rozwój cyfryzacji życia społecznego, a także powszechna dostępność Internetu, doprowadziły do zasadniczej zmiany w sposobie korzystania z utworów muzycznych. Zmiany na rynku muzycznym, które rozpoczęły się na początku XXI wieku, a przyspieszyły wraz z rozwojem usług *streamingowych*, spowodowały przejście od modelu nabywania egzemplarzy utworów do modelu opierającego się na dostępie do nich. Jak wynika z danych Międzynarodowej Federacji Przemysłu Fonograficznego (IFPI) *streaming* obecnie generuje 69% przychodów w branży muzycznej, a fizyczne nośniki takie jak płyty CD czy winylowe jedynie 16,4%. Zgodnie z raportem IFPI *Global Music Report 2025* (za rok 2024), w ramach *streamingu* segment subskrypcyjny wzrósł o 9,5 %. Liczba użytkowników płatnych subskrypcji *streamingu* osiągnęła 752 miliony. Jak wynika z przytoczonych danych *streaming* stał się nie tylko główną formą słuchania muzyki, ale wręcz podstawą współczesnego rynku fonograficznego[1].

Ten proces wiąże się jednak z trwale rozwijającym się problemem piractwa w sieci. Pomimo dużej dostępności legalnych źródeł korzystania z muzyki, piractwo stanowi wciąż spore wyzwanie dla ochrony praw autorskich. Z tradycyjnego kopiowania fizycznych nośników piractwo muzyczne przekształciło się w szereg zaawansowanych pod względem technicznym praktyk, takich jak udostępnianie za pomocą sieci *peer-to-peer*[2], *stream-ripping*, wykorzystywanie fragmentów utworów w mediach społecznościowych, a także wykorzystywanie muzyki poprzez systemy sztucznej inteligencji. Zgodnie z raportem Europejskiego Urzędu ds. Własności Intelektualnej (EUIPO) na koniec roku 2023 w stosunku do roku 2022 piractwo muzyczne wzrosło do 0,64 dostępu na użytkownika Internetu miesięcznie, a główną metodę dostępu do pirackiej muzyki stanowi *ripping*, polegający na pobieraniu treści strumieniowych[3]. Piractwo muzyczne w sieci ciągle ewoluuje, stanowiąc złożony i trudny do monitorowania oraz zwalczania problem, czego skutki odczuwa cały sektor muzyczny.

[1] IFPI, *Global Music Report 2025*. State of the Industry, s. 4-11.
[2] S. Blichiewicz, *Problem piractwa muzycznego: alternatywne spojrzenie na spór o pobieranie muzyki z Internetu, [w:] Media-Kultura-Komunikacja Społeczna*, Uniwersytet Warmińsko-Mazurski w Olsztynie, Olsztyn 2013, s. 192-208.
[3] EUIPO, *Online Copyright Infringement in the EU. Full Report 2024, s. 42.*

Celem niniejszego artykułu jest analiza zjawiska piractwa muzycznego w sieci jako współczesnego zagrożenia dla ochrony praw autorskich, a także wskazanie związanych z nim konsekwencji prawnych. W opracowaniu omówiona zostanie istota piractwa w sieci w kontekście utworów muzycznych oraz typowe współcześnie praktyki naruszające prawa autorskie. Ponadto zostanie dokonana analiza odpowiedzialności zarówno użytkowników, jak i platform internetowych. W pracy pozostaną również wskazane obecne metody przeciwdziałania piractwu muzycznemu w sieci. Tak zakreślony cel pozwala zauważyć kluczowe problemy związane z piractwem muzycznym w sieci oraz podjąć próbę oceny obowiązujących regulacji.

2. Piractwo w sieci w świetle prawa autorskiego

„Piractwo" jest jedną z najczęściej występujących form cyberprzestępczości, jednak mimo powszechności, pojęcie to nie posiada jednolitej definicji legalnej i stanowi określenie potoczne. Zgodnie z doktryną, piractwo jest czerpaniem korzyści z rozpowszechniania utworów bez zgody uprawnionego podmiotu oraz bez zapłaty należnego wynagrodzenia[4]. Warto zwrócić uwagę, że piractwo intelektualne odnosi się do wszelkich naruszeń praw własności intelektualnej, co obejmuje także patenty czy bazy danych[5]. Natomiast piractwo intelektualne dokonywane w środowisku internetowym określane jest mianem piractwa internetowego. Polega ono na nielegalnym kopiowaniu, udostępnianiu w sieci własności intelektualnej, a także dostarczaniu oprogramowania, które służy łamaniu zabezpieczeń oraz czerpaniu z tego tytułu korzyści. Piractwem internetowym nazywa się więc nielegalne kopiowanie bez uzyskania zgody twórcy oraz wniesienia określonych opłat, a także słuchanie czy oglądanie plików *online* o nielegalnym pochodzeniu[6].

Na potrzeby dalszej analizy niezbędne jest wyjaśnienie pojęcia utworu muzycznego. Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych[7] (dalej: PrAut) nie zawiera odrębnej definicji utworu muzycznego, zaliczając go do ogólnej kategorii

[4] R. Golat, *Prawo autorskie i prawa pokrewne*, Warszawa 2014, s. 228.
[5] J. Sobczyk, K. Chałubińska-Jentkiewicz, M. Nowikowska, *Piractwo w sieci*, Poznań 2022, s. 49.
[6] Ibidem, s. 56.
[7] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (t.j. Dz. U. z 2025 r. poz. 24 z późn. zm.) (dalej: PrAut).

„utworu”. Zgodnie z art. 1 ust. 1 PrAut, utworem jest każdy przejaw twórczej działalności człowieka o indywidualnym charakterze, utrwalony w jakiejkolwiek postaci, niezależnie od jego wartości, przeznaczenia czy sposobu wyrażenia. Ochrona prawnoautorska powstaje już z momentem ustalenia utworu, nawet jeśli nie został on jeszcze ukończony, i nie jest uzależniona od spełnienia jakichkolwiek formalności, takich jak rejestracja czy zgłoszenie[8].

Z punktu widzenia prawa autorskiego piractwo należy zakwalifikować przede wszystkim jako naruszenie autorskich praw majątkowych przysługujących twórcy lub innym uprawnionym podmiotom. Zgodnie z art. 17 PrAut, jeżeli ustawa nie stanowi inaczej, twórcy przysługuje wyłączne prawo do korzystania z utworu i rozporządzania nim na wszystkich polach eksploatacji oraz do wynagrodzenia za korzystanie z utworu. Naruszenia związane z piractwem, w szczególności nielegalne zwielokrotnianie, udostępnianie oraz pobieranie utworów z nieautoryzowanych źródeł, ingerują właśnie w sferę majątkowych uprawnień twórcy, polegających na wyłączności eksploatacji utworu i czerpaniu z niego korzyści majątkowych. Naruszenie autorskich praw majątkowych rozumie się jako korzystanie z utworu lub jego twórczych elementów bez zgody podmiotu uprawnionego lub bez istnienia ustawowej podstawy takiego korzystania, wynikającej z przepisów o dozwolonym użytku[9]. Należy jednak zauważyć, iż w pewnych sytuacjach działania o charakterze pirackim mogą dotykać także autorskich praw osobistych twórcy, na przykład poprzez usuwanie oznaczenia autorstwa czy naruszenie integralności utworu.

Instytucja dozwolonego użytku prywatnego stanowi wyjątek od zasady prawnoautorskiego monopolu. Została uregulowana w art. 23 PrAut, z którego wynika, że bez zezwolenia twórcy wolno nieodpłatnie korzystać z już rozpowszechnionego utworu w zakresie własnego użytku osobistego. Zakres podmiotowy dozwolonego użytku prywatnego, obejmuje korzystanie z pojedynczych egzemplarzy utworów przez osoby pozostające w związkach osobistych, w szczególności na podstawie pokrewieństwa, powinowactwa bądź stosunku towarzyskiego[10]. Postać korzystania nie jest przy tym

[8] J. Barta, et al., *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2001, s.5.
[9] A. Matlak, T. Targosz, E. Traple [w:] *Komentarz do ustawy o prawie autorskim i prawach pokrewnych [w:] Ustawy autorskie. Komentarze. Tom II*, red. R. Markiewicz, Warszawa 2021, art. 79.
[10] P. Chmielnicka, *Dozwolony użytek prywatny a serwisy streamingowe w świetle prawa autorskiego, [w:] Internet a prawo autorskie, red. A. Niewęgłowski, M. Chrzanowski*, Lublin 2016, s. 23-24.

ograniczona, co oznacza, że może dotyczyć wszystkich pól eksploatacji utworu, w tym jego zwielokrotniania w formie cyfrowej oraz dowolnych sposobów rozpowszechniania[11]. Podstawową przesłanką legalności korzystania z utworu w ramach dozwolonego użytku prywatnego jest jego wcześniejsze rozpowszechnienie. Kolejnym warunkiem korzystania z utworu w omawianym zakresie jest jego nieodpłatny i ściśle osobisty charakter[12]. Należy zauważyć, że z dyspozycji art. 23 PrAut nie wynika wprost wymóg legalności źródła. Kwestia ta została jednak rozstrzygnięta w wyroku Trybunału Sprawiedliwości w sprawie *ACI Adam BV i in.*[13], w którym uznano za niedopuszczalne uregulowanie nierozróżniające legalności źródła utworu. W konsekwencji dozwolony użytek prywatny ogranicza się wyłącznie do korzystania z utworów pochodzących z legalnych źródeł[14].

3. Współczesne formy piractwa utworów muzycznych

Muzyka, która przez wiele lat była związana jedynie z materialnymi nośnikami, obecnie funkcjonuje przede wszystkim jako zapis cyfrowy dostępny w środowisku sieciowym. Proces digitalizacji doprowadził do „oderwania" utworu muzycznego od fizycznego nośnika i przekształcenia go w zbiór danych, które mogą być praktycznie nieskończenie zwielokrotniane. Jak wskazuje Stanisław Jędrzejewski, kluczowym momentem w tym procesie było upowszechnienie formatu MP3 oraz rozwój Internetu szerokopasmowego, które umożliwiły łatwe kopiowanie i przesyłanie plików muzycznych między użytkownikami na masową skalę. Następnie pojawienie się technologii wymiany plików typu *peer-to-peer* oraz platform internetowych doprowadziło do przekształcenia tradycyjnego modelu dystrybucji muzyki w model oparty na dostępie, a nie posiadaniu. Zmiana ta zasadniczo wpłynęła zarówno na rynek muzyczny, jak i na pozycję odbiorcy, który z biernego słuchacza stał się aktywnym uczestnikiem obiegu treści. Utwory muzyczne w sieci charakteryzują się więc niematerialnym charakterem, łatwością kopiowania oraz globalnym zasięgiem udostępniania[15].

[11] Ibidem.
[12] P. Chmielnicka, *op.cit.* s. 24-25.
[13] Wyrok TS z dnia 10.04.2014 r., C-435/12, ACI Adam BV i in. v. Stichting de Thuiskopie i Stichting Onderhandelingen Thuiskopie vergoeding (EU:C:2014:254),
[14] J. Sobczyk, K. Chałubińska-Jentkiewicz, M. Nowikowska, *op.cit.*, s. 128-129.
[15] S. Jędrzejewski, *Od muzyki w radiu do muzyki w sieci* [w:] „Kultura współczesna" 3(96)/2017.

Od lat jedną z najbardziej rozpowszechnionych form piractwa muzycznego w sieci jest technologia *peer-to-peer*, która umożliwia szybką i niemal anonimową wymianę plików pomiędzy użytkownikami[16]. W odróżnieniu od sytuacji, w której pliki są ściągane z serwerów, system *peer-to-peer* działa na zasadzie sieci równorzędnej, w której każdy może komunikować się z każdym. Opiera się na bezpośredniej wymianie danych cyfrowych pomiędzy użytkownikami. Ta technologia daje możliwość odnalezienia pliku na innym komputerze i skopiowania jego zakodowanych danych na własny dysk twardy[17].
Zgodnie z raportem IFPI *Engaging with Music 2023* najpowszechniejszą formą internetowego naruszania praw autorskich w muzyce jest *stream-ripping*[18], który można określić jako nielegalne zgrywanie utworów muzycznych bezpośrednio z kanałów strumieniowych[19]. Zjawisko to polega na „zgrywaniu" na twardy dysk komputera muzyki udostępnionej w Internecie za pomocą techniki *streamingu*[20]. Wśród serwisów najczęściej wykorzystywanych do nielegalnego pozyskiwania muzyki dominują platformy o największej popularności takie jak *YouTube Music* czy *Spotify*[21].

Kolejną rozpowszechnioną formą piractwa muzycznego są serwisy internetowe oraz aplikacje, które bez wymaganych licencji umożliwiają strumieniowe odtwarzanie muzyki. W odróżnieniu od legalnych źródeł, takie serwisy nie podpisują umów z organizacjami zbiorowego zarządzania ani z podmiotami posiadającymi prawa autorskie, a ich działalność skupia się wyłącznie na zysku, finansowanym przez reklamy, płatne subskrypcje czy inne metody zarabiania[22].

Specyficzną formą naruszania praw autorskich w sieci jest piractwo w mediach społecznościowych. Polega ono na wykorzystywaniu utworów muzycznych przez użytkowników zazwyczaj jako tła dźwiękowego do krótkich form audiowizualnych takich jak treści publikowane na platformach typu *TikTok, Instagram (reels),* czy *YouTube Shorts*. Użytkownicy publikując materiały często korzystają jedynie z wybranych fragmentów

[16] S. Blichiewicz, *op.cit.*, s. 192-193.
[17] J. Sobczyk, K. Chałubińska-Jentkiewicz, M. Nowikowska, *op.cit.* s. 56-57.
[18] IFPI, *Engaging with Music 2023 - Full Raport*, 2023, s. 22-23.
[19] M. Szczyrba, *Jak przemysł 4.0 ograniczył cyfrowe piractwo w świecie muzyki [w:] Interdyscyplinarne badania młodych naukowców*, red. B. Balon, Gliwice 2024, s. 558.
[20] Raport Deloitte, *Piractwo w Internecie - straty dla kultury i gospodarki. Analiza wpływu zjawiska piractwa internetowego na gospodarkę Polski na wybranych rynkach kultury*, Warszawa 2017, s. 118.
[21] M. Szczyrba, *op.cit.*, s. 558.
[22] J. Koćwin, *Portale społecznościowe do wymiany plików a piractwo medialne,* Wrocław 2018, s. 160-161.

utworów muzycznych, czego skutkiem jest ich oderwanie od utworu pierwotnego, czyli fragmentaryzacja. Mimo, że większość serwisów społecznościowych posiada licencje na dany zbiór utworów, a także udostępnia informacje dotyczące aktualnych praw autorskich, rzeczywiste zachowania użytkowników często przekraczają dozwolone granice[23].

Nową i złożoną formą piractwa muzycznego jest stosowanie sztucznej inteligencji do tworzenia utworów, które naśladują styl określonych artystów zwane *AI-covery*. Modele sztucznej inteligencji są w tym celu szkolone na istniejących, chronionych utworach muzycznych, co rodzi poważne wątpliwości prawne. W rezultacie powstają nowe nagrania, które odwzorowują charakterystyczne cechy głosu, kompozycji czy styl artysty. Modele do tworzenia *AI-coverów* umożliwiają użytkownikom wykorzystywanie głosu piosenkarza w dowolnych utworach, z których część jest tworzona masowo i charakteryzuje się niską jakością. W praktyce tego rodzaju utwory są publikowane i rozpowszechniane w sieci, często z oznaczeniem sugerującym udział konkretnego twórcy[24].

4. Odpowiedzialność prawna za piractwo muzyczne

Piractwo internetowe współcześnie rozumiane jest głównie jako nieuprawnione rozpowszechnianie utworów chronionych prawem autorskim[25]. Zwalczanie zjawiska piractwa w sieci ma zapewnić przede wszystkim art. 116 ust. 1 PrAut, który stanowi, że „kto bez uprawnienia albo wbrew jego warunkom rozpowszechnia cudzy utwór w wersji oryginalnej albo w postaci opracowania, artystyczne wykonanie, fonogram, wideogram lub nadanie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2". Przepis ten ustanawia karnoprawną ochronę majątkowych praw autorskich i jest ukierunkowany na przeciwdziałanie zjawisku piractwa, polegającego na nieuprawnionym

[23] M. Gwioździk, *Prawo własności intelektualnej w muzyce i choreografii (na przykładzie wybranych mediów społecznościowych),* Warszawa 2024, s. 517-517-522.
[24] Jingwen, J., *Copyrights Infringement Risks in AI-generated Cover Songs: An Analysis Based on Current Legislation*, School of Law, Beijing Foreign Studies University, Pekin.
[25] *Z. Ćwiąkalski, Prawo autorskie i prawa pokrewne. Komentarz*, pod red. *J. Barty, R. Markiewicza*, Warszawa 2011, s. 745.

rozpowszechnianiu cudzych utworów bez ponoszenia kosztów związanych z legalnym korzystaniem z przedmiotów ochrony prawa autorskiego[26].

Dla istnienia przestępstwa z art. 116 PrAut nie ma znaczenia, czy utwory były udostępniane przez platformę, która automatycznie usuwa pliki po pewnym czasie, ani też to, czy inne osoby rzeczywiście je pobrały. Te okoliczności mogą jedynie wpływać na wymiar kary orzekanej przez sąd. Podobnie bez znaczenia dla odpowiedzialności karnej pozostaje podział plików na części, ich kompresja do innych formatów czy zamieszczanie przez udostępniających komunikatów nakazujących usunięcie plików po określonym czasie od pobrania[27].

Niezależnie od odpowiedzialności karnej, roszczeń można dochodzić również na drodze cywilnej. W sytuacji naruszenia autorskich praw majątkowych, po stronie uprawnionego powstaje możliwość dochodzenia roszczeń przewidzianych w art. 79 PrAut, które obejmują w szczególności żądanie zaniechania naruszeń oraz usunięcia ich skutków, a także naprawienia wyrządzonej szkody. Odpowiedzialność ta może być realizowana na zasadach ogólnych prawa cywilnego albo poprzez zapłatę stosownej kwoty pieniężnej odpowiadającej dwukrotności należnego wynagrodzenia, które byłoby właściwe za udzielenie zgody na korzystanie z utworu, natomiast w przypadku zawinionego naruszenia, trzykrotności takiego wynagrodzenia. Niezależnie od tego uprawnionemu przysługuje również roszczenie o wydanie bezprawnie uzyskanych korzyści[28]. Natomiast zgodnie z art. 78 PrAut twórca, którego osobiste prawa autorskie zostały zagrożone czy naruszone, może żądać zaprzestania takiego działania. Jeśli naruszenie już nastąpiło, może również domagać się, aby osoba, która dopuściła się naruszenia, wykonała odpowiednie czynności zmierzające do usunięcia skutków, w szczególności publicznego oświadczenia o odpowiedniej treści i formie. Gdy doszło do zawinionego naruszenia, twórca może otrzymać rekompensatę pieniężną za doznaną

[26] J. Sobczyk, K. Chałubińska-Jentkiewicz, M. Nowikowska, *op.cit.*, s. 95-96.
[27] Ibidem.
[28] I. Drożdż, K. Sączek, *Dozwolony użytek osobisty w Internecie a problem torrentów* [w:] Internetowy Przegląd Prawniczy TBSP UJ 2016/4, Kraków 2016, s. 67.

krzywdę, a na jego wniosek sąd może nakazać sprawcy przekazanie określonej sumy na wskazany cel społeczny[29].

Istotną zmianę w zakresie odpowiedzialności za nielegalne treści w środowisku cyfrowym wprowadziła Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 tzw. dyrektywa DSM[30], a w szczególności jej art. 17. Regulacja ta nakłada na dostawców usług udostępniania treści *online* powinność podejmowania działań zmierzających do weryfikacji materiałów jeszcze przed ich publicznym rozpowszechnieniem. Zgodnie z tym przepisem, dostawca usług powinien uzyskać od podmiotów uprawnionych stosowne zezwolenie, na przykład w drodze zawarcia umowy licencyjnej. W sytuacji, gdy dochodzi do udostępnienia utworu objętego ochroną prawa autorskiego, to na dostawcy platformy ciąży obowiązek wykazania, że dołożył należytej staranności zarówno w celu uzyskania takiego zezwolenia, jak i w celu uniemożliwienia dostępu do utworów oraz innych przedmiotów ochrony, co do których uprawnieni przekazali mu istotne i wystarczające informacje. Dodatkowo dostawca usług *online* musi udowodnić, że po otrzymaniu należycie uzasadnionego zgłoszenia od podmiotu uprawnionego niezwłocznie podjął działania mające na celu zablokowanie dostępu do kwestionowanych treści lub ich usunięcie z platformy, a także że wdrożył odpowiednie środki techniczne i organizacyjne służące zapobieganiu ich ponownemu zamieszczeniu w przyszłości[31]. Rozwiązania przewidziane w art. 17 dyrektywy DSM zostały implementowane do polskiego porządku prawnego w postaci Oddziału 21 rozdziału 6^1 PrAut, zatytułowanego „Dostawcy usług udostępniania treści online".

5. Skutki nielegalnego korzystania z muzyki online oraz sposoby jego ograniczania

Piractwo cyfrowe może wywoływać długofalowe negatywne konsekwencje zarówno dla twórców, jak i dla podmiotów działających na rynku fonograficznym. Przede wszystkim prowadzi ono do redukcji przychodów uzyskiwanych z legalnej dystrybucji utworów.

[29] A. Mazur, K. Cichoń, *Utwór muzyczny w Internecie a prawo autorskie* [w:] Internet a prawo autorskie, Lublin 2016, s.62.

[30] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. U. UE. L. z 2019 r. Nr 130, str. 92).

[31] E. Dziuba, *Konstytucja internetu a własność intelektualna - Jak Akt o usługach cyfrowych chroni dobra niematerialne?* [w:] Prawo Mediów Elektronicznych. Kwartalnik Naukowy 2024, nr 3, s. 38-39.

Oddziaływanie nie ogranicza się jednak wyłącznie do sfery finansowej, piractwo, zwłaszcza w formie fragmentarycznego wykorzystywania utworów, ich przeróbek oraz rozpowszechniania bez oznaczenia autorstwa, prowadzi do naruszenia osobistych praw autorskich. Zjawisko to może również osłabiać potencjał twórczy i innowacyjność branży muzycznej[32]. Piractwo niesie za sobą także ryzyko naruszenia wizerunku i pozycji rynkowej twórców oraz wytwórni. Nieautoryzowane rozpowszechnianie utworów skutkuje utratą kontroli nad kanałami dystrybucji oraz sposobem prezentacji muzyki, co może wpływać negatywnie na strategie promocyjne i sprzedażowe[33].

Odpowiedzią na zjawisko piractwa muzycznego w sieci są kompleksowe działania zapobiegawcze, podejmowane na gruncie prawnym, technologicznym i edukacyjnym.

Kluczowe znaczenie mają regulacje prawne, w szczególności przepisy dotyczące odpowiedzialności za nielegalne rozpowszechnianie utworów. Istotną rolę odgrywają również rozwiązania wynikające z art. 17 dyrektywy DSM, implementowane do polskiego porządku prawnego w ramach przepisów dotyczących dostawców usług udostępniania treści *online*, które znacząco rozszerzają odpowiedzialność platform internetowych za treści zamieszczane przez użytkowników.

Równolegle współczesne technologie oferują nowoczesne procedury między innymi *notice and take down*, która polega na obowiązku usunięcia nielegalnej treści przez podmiot, który został o niej poinformowany, pod rygorem odpowiedzialności prawnej. Mechanizm ten ma jednak ograniczoną skuteczność, gdyż usunięte materiały często pojawiają się ponownie pod innymi adresami URL, co wymusza stały i czasochłonny monitoring ze strony podmiotów uprawnionych. Odpowiedzią na tę niedoskonałość jest mechanizm *notice and stay down*, przewidziany w dyrektywie DSM, który zobowiązuje platformy do zapobiegania ponownemu udostępnianiu raz zgłoszonych treści naruszających prawo[34].

Coraz większe znaczenie zyskują instrumenty ekonomiczne, realizowane zgodnie z koncepcją *follow the money*, których celem jest ograniczenie opłacalności działalności

[32] https://www.muso.com/piracy-in-the-music-industry (dostęp z: 28.11.2025 r.)
[33] Ibidem.
[34] Raport Deloitte, *Kradzież treści wideo w internecie, Analiza wpływu zjawiska piractwa internetowego treści audiowizualnych, w tym telewizyjnych na gospodarkę Polski,* Warszawa 2023, s. 68.

piracкiej. Działania te polegają na odcinaniu serwisów pirackich od źródeł finansowania poprzez blokowanie wpływów z reklam oraz uniemożliwianie dokonywania płatności za dostęp do nielegalnych treści. W tym celu wykorzystywane są m.in. tzw. „czarne listy" domen, udostępniane przez Stowarzyszenie „Sygnał" partnerom z sektora reklamowego i mediowego. Równolegle nawiązywana jest współpraca z bankami i operatorami płatności elektronicznych, co utrudnia piratom korzystanie z tradycyjnych systemów płatności i zmusza ich do stosowania mniej akceptowanych przez użytkowników rozwiązań, takich jak kryptowaluty[35].

Także podmioty poszkodowane przez piractwo w Internecie podejmują szereg działań o charakterze prewencyjnym i interwencyjnym w celu ochrony swoich treści. Obejmują one zarówno czynności zautomatyzowane, realizowane w ramach sformalizowanych procedur przeciwdziałania naruszeniom, jak i działania manualne, polegające przede wszystkim na stałym monitorowaniu przestrzeni internetowej pod kątem nieautoryzowanych transmisji oraz nielegalnego udostępniania treści. Aktywność ta ma na celu szybkie identyfikowanie przypadków naruszeń i inicjowanie dalszych działań zmierzających do ich usunięcia[36].

Równolegle istotną rolę pełnią instrumenty instytucjonalne i edukacyjne. Przykładem jest działalność Stowarzyszenia „Sygnał", które nie tylko koordynuje działania branżowe, ale również prowadzi liczne projekty szkoleniowe[37].

6. Podsumowanie

Dynamiczny rozwój nowoczesnych technologii cyfrowych zasadniczo wpłynął na sposoby tworzenia, dystrybucji i odbierania muzyki, jednocześnie generując nowe wyzwania związane z ochroną praw autorskich. Piractwo w sieci, mimo wzrostu popularności legalnych usług *streamingowych* oraz rozbudowy instrumentów prawnych, nadal pozostaje poważnym problemem dla całego sektora muzycznego. Współczesne formy piractwa stają się coraz bardziej zróżnicowane i trudniejsze do zwalczenia, co jest

[35] Ibidem, s. 69.
[36] Ibidem, s. 70.
[37] Ibidem.

efektem zarówno postępu technologicznego, jak i międzynarodowego, anonimowego charakteru środowiska internetowego.

Przeprowadzona analiza pokazuje, że zasady dotyczące ochrony uległy wielu zmianom wraz z rozwojem Internetu i zapewne będą dalej ewoluować. Szczególne znaczenie ma w tym zakresie implementacja art. 17 dyrektywy DSM do polskiego porządku prawnego, która doprowadziła do przesunięcia ciężaru odpowiedzialności z indywidualnych użytkowników na platformy cyfrowe. Niemniej jednak praktyka pokazuje, że prawo często nie nadąża za tempem rozwoju technologii, zwłaszcza w kontekście nowych form eksploatacji muzyki i naruszeń dokonywanych w sposób zautomatyzowany lub transgraniczny.

Prawo związane z przestrzenią internetową musi pozostać elastyczne oraz proporcjonalne. Stanowi to wyzwanie dla prawodawców zarówno na poziomie międzynarodowym i krajowym, lecz cyberprzestrzeń nie może być miejscem, w którym prawo nie ma zastosowania[38]. Skuteczna ochrona muzyki w środowisku cyfrowym wymaga współpracy twórców, platform internetowych oraz ustawodawcy, a także dostosowania istniejących regulacji do dynamicznie zmieniającej się rzeczywistości technologicznej.

Bibliografia

Barta J., Czajkowska-Dąbrowska M., Ćwiąkalski Z., Markiewicz R., Traple A., *Ustawa o prawie autorskim i prawach pokrewnych. Komentarz*, Warszawa 2001.

Blichiewicz S., *Problem piractwa muzycznego: alternatywne spojrzenie na spór o pobieranie muzyki z Internetu*, [w:] *Media–Kultura–Komunikacja Społeczna*, UWM, Olsztyn 2013.

Chmielnicka P., *Dozwolony użytek prywatny a serwisy streamingowe w świetle prawa autorskiego*, [w:] *Internet a prawo autorskie*, red. A. Niewęgłowski, M. Chrzanowski, Lublin 2016.

Ćwiąkalski Z., *Prawo autorskie i prawa pokrewne. Komentarz*, red. J. Barta, R. Markiewicz, Warszawa 2011.

Drożdż I., Sączek K., *Dozwolony użytek osobisty w Internecie a problem torrentów*, „Internetowy Przegląd Prawniczy TBSP UJ" 2016/4, Kraków 2016.

Dziuba E., *Konstytucja internetu a własność intelektualna - Jak Akt o usługach cyfrowych chroni dobra niematerialne? [w:]* Prawo Mediów Elektronicznych. Kwartalnik Naukowy 2024, nr 3

[38] J. Worona, *1.2. Koncepcja nowego ładu cyberprzestrzeni*, [w:] J. Worona, Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Warszawa 2020, s. 424

Golat R., *Prawo autorskie i prawa pokrewne*, Warszawa 2014.

Gwioździk M., *Prawo własności intelektualnej w muzyce i choreografii*, Warszawa 2024.

Jędrzejewski S., *Od muzyki w radiu do muzyki w sieci*, „Kultura Współczesna" 2017, nr 3(96).

Jingwen J., *Copyrights Infringement Risks in AI-generated Cover Songs*, School of Law, Beijing Foreign Studies University, Pekin.

Koćwin J., *Portale społecznościowe do wymiany plików a piractwo medialne*, Wrocław 2018.

Matlak A., Targosz T., Traple E., *Komentarz do ustawy o prawie autorskim i prawach pokrewnych*, [w:] *Ustawy autorskie. Komentarze*, t. II, red. R. Markiewicz, Warszawa 2021.

Mazur A., Cichoń K., *Utwór muzyczny w Internecie a prawo autorskie*, [w:] Internet a prawo autorskie, Lublin 2016.

Sobczyk J., Chałubińska-Jentkiewicz K., Nowikowska M., *Piractwo w sieci*, Poznań 2022.

Szczyrba M., *Jak przemysł 4.0 ograniczył cyfrowe piractwo w świecie muzyki*, [w:] *Interdyscyplinarne badania młodych naukowców*, red. B. Balon, Gliwice 2024.

Worona J., *1.2. Koncepcja nowego ładu cyberprzestrzeni*, [w:] J. Worona, Cyberprzestrzeń a prawo międzynarodowe. Status quo i perspektywy, Warszawa 2020.

Akty prawne i orzeczenia

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2019/790 z dnia 17 kwietnia 2019 r. w sprawie prawa autorskiego i praw pokrewnych na jednolitym rynku cyfrowym oraz zmiany dyrektyw 96/9/WE i 2001/29/WE (Dz. U. UE. L. z 2019 r. Nr 130, str. 92).

Ustawa z 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U. 2025, poz. 24).

Wyrok TS z dnia 10.04.2014 r., C-435/12, ACI Adam BV i in. v. Stichting de Thuiskopie i Stichting Onderhandelingen Thuiskopie vergoeding (EU:C:2014:254).

Źródła internetowe i raporty

Deloitte, *Kradzież treści wideo w internecie. Analiza wpływu zjawiska piractwa treści audiowizualnych na gospodarkę Polski*, Warszawa 2023.

Deloitte, *Piractwo w Internecie - straty dla kultury i gospodarki*, Warszawa 2017.

EUIPO (European Union Intellectual Property Office), *Online Copyright Infringement in the EU. Full Report 2024*.

IFPI, *Engaging with Music 2023 - Full Report*, 2023.

IFPI, *Global Music Report 2025. State of the Industry*.

Muso.com, „Piracy in the music industry", https://www.muso.com/piracy-in-the-music-industry (dostęp z: 28.11.2025).

„dot.pl" - czasopismo Rejestru domeny .pl

Criminal liability for the offence of disrupting the functioning of an IT network

Filip Mikołaj Radoniewicz
Wydział Nauk Społecznych, Instytut Nauk o Polityce i Bezpieczeństwie, Zakład Praw Człowieka, University of Rzeszów, Poland
ORCID: https://orcid.org/0000-0002-7917-4059
E-mail: filip.radoniewicz@radoniewicz.eu

Abstract

The article discusses the issue of computer crimes (cybercrimes) involving the disruption of the functioning of ICT networks.

Objective: To assess the criminal law provisions in force in Poland concerning attacks on data and information systems (Articles 268a, 269, 269a of the Penal Code) and to identify their inconsistencies and the legislative changes needed.

Methods: The author conducts a dogmatic analysis of the provisions, compares their content with practical interpretative problems, contrasts them with EU regulations (Directive 2013/40) and the Convention on Cybercrime, and refers to doctrinal viewpoints.

Conclusions: The provisions overlap, are imprecise, and are inadequate in light of contemporary threats. Articles 268a and 269a partially duplicate each other, while Articles 268 §2 and 269 §2 are unnecessary. It is essential

Received: 07.12.2025
Accepted: 19.12.2025
Published: 19.12.2025

Cite this article as:
F. Radoniewicz, "*Criminal liability for the offence of disrupting the functioning of an IT network*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/215838

Corresponding author:
Filip Radoniewicz, Wydział Nauk Społecznych, Instytut Nauk o Polityce i Bezpieczeństwie, Zakład Praw Człowieka, University of Rzeszów, Poland
E-mail: filip.radoniewicz@radoniewicz.eu

to clarify the scope of protection for data and systems, to organize the relationships between the relevant articles, and to increase penalties for attacks on critical infrastructure so that Polish law meets the requirements of Directive 2013/40 and the realities of cybersecurity.

Keywords: IT network, information system, Convention on Cybercrime, directive 2013/40

Introduction

Crimes involving the disruption of the functioning of IT systems and ICT networks are defined in Articles 268a, 269 and 269a of the Penal Code, in Chapter XXXIII of the Penal Code, entitled "Offences against the Protection of Information."[1]According to Article 268a §1 of the Penal Code, anyone who, without authorization, destroys, damages, deletes, alters, or hinders access to computer data, or who significantly disrupts or prevents the automatic processing, storage, or transmission of such data[2], is subject to a penalty of imprisonment for up to three years. The object of protection in this provision is computer data—specifically, their integrity (i.e., protection against destruction, damage, or deletion) and their availability (secure storage, processing, and transmission by authorized persons). Computer programs are also protected, as the legislator uses the term "computer data" rather than "information," as in Article 268 of the Penal Code[3].

[1] The Act of 6 June 1997 – Penal Code (Journal of Laws of 2025, item 383, as amended), hereinafter referred to as the Penal Code (k.k.).

[2] In light of Article 2(b) of Directive 2014/30, the term "computer data" should be understood as "a representation of facts, information or concepts in a form suitable for processing in an information system, including a program capable of causing an information system to perform a function." A similar definition appears in the Council of Europe Convention on Cybercrime of 23 November 2001 (Journal of Laws of 2015, item 728). According to these definitions, computer data constitute a medium for information, facts, and concepts, which become readable to a computer (or information) system only once they are converted into the form of computer data.

[3] Similarly, P. Kozłowska-Kalisz (P. Kozłowska-Kalisz, in: M. Mozgawa (ed.), *Penal Code. Practical Commentary*, Wolters Kluwer, LEX/el. 2025, Commentary on Article 268a, para. 2) and M. Siwicki, who additionally points to the proper functioning of computer programs—which in essence falls within the scope of "data integrity" (M. Siwicki, *Cybercrime*, C.H. Beck, Warsaw 2013, p. 147). However, there is no consensus in the doctrine on this matter. Andrzej Adamski argues that Article 268a of the Penal Code protects only the availability of data (see A. Adamski, *Cybercrime – Legal and Criminological Aspects*, "Studia Prawnicze" 2005/4, pp. 58–59), which follows from his interpretation of this provision. Włodzimierz Wróbel and Dominik Zając refer more broadly to "the security of information stored, transmitted, and processed in systems operating on the basis of computer data" (W. Wróbel,

D. Zając, in: W. Wróbel, A. Zoll (eds.), *Criminal Code. Special Part. Volume II. Part II. Commentary on Articles 212–277d*, Wolters Kluwer, Warsaw 2017, Commentary on Article 268a, para. 1). By contrast, J. Giezek and B. Kunicka-Michalska (J.W. Giezek, in: J.W. Giezek (ed.), *Criminal Code. Special Part. Commentary*, Wolters Kluwer, Warsaw 2021, LEX/el., Commentary on Article 268a, para. 1; B. Kunicka-Michalska, in: L. Gardocki (ed.), *System of Criminal Law, Vol. 8: Offences Against the State and Collective Goods*, C.H. Beck, Warsaw 2018, p. 1031) present the position that, in addition to the integrity and availability of computer data, Article 268a of the Penal Code also protects their confidentiality—a view which, in my opinion, belongs to the domain of Articles 267 §1–4 of the Penal Code.

The legislator did not use in this provision the terms “computer (information) system”[4], “ICT system”[5], or “telecommunications[6] or teleinformatics network”[7].

[4]The interpretation of this concept has posed problems essentially since its introduction into the Penal Code (see, for example, F. Radoniewicz, *Criminal Liability for Hacking and Other Offences Against Computer Data and Information Systems*, Wolters Kluwer, Warsaw 2016, pp. 275–278), problems which intensified further after Poland ratified the Convention on Cybercrime. Since Article 267 §2 of the Penal Code was added through a 2008 amendment (Act of 24 October 2008 amending the Penal Code and certain other acts; Journal of Laws No. 214, item 1344), linked to the implementation of Council Framework Decision 2005/222/JHA on attacks against information systems (OJ EU 2005 L 69/67), it would be advisable to interpret this term in accordance with the definition in that instrument and in the subsequent Directive 2013/40—namely, as both a single device that processes computer data and a group of interconnected devices, i.e., a network. Pursuant to Article 2(b) of the Directive, this is “a device or group of interconnected or related devices, one or more of which, in accordance with a program, performs automatic processing of computer data, as well as computer data stored, processed, retrieved, or transmitted by that device or group of devices, for their operation, use, protection, or maintenance.” However, numerous errors were made in translating the text of the Convention on Cybercrime. One such error was translating the term *computer system* as *information system*. The substantive scope of the term *computer system* in the Convention is narrower than that of “information system” under Directive 2013/40 (despite similarities in their definitions). According to Article 1(a) of the Convention, a computer system is defined as “any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.” (See extensively: F. Radoniewicz, *Criminal Liability...*, pp. 166–167, 244–249.) This mistranslation generates uncertainty regarding the scope of the term “information system” under the Penal Code.
It should also be noted that although the Convention on Cybercrime became part of the Polish legal order upon ratification, the definition of “information (computer) system” cannot be applied directly due to the problems discussed above. The confusion is compounded by the fact that, in the translation of the definition of “computer data” in Article 2(b) of the Convention (translated as “informatic data”), the term *computer system* is used (“computer data means any representation of facts, information, or concepts in a form suitable for processing in a computer system, including an appropriate program enabling the information system to perform a function”). Moreover, the term “computer system” appears in the translation of the Additional Protocol to the Council of Europe Convention on Cybercrime concerning the criminalisation of acts of a racist or xenophobic nature committed through computer systems of 28 January 2003 (Journal of Laws 2015, item 730).

[5] Pursuant to Article 2 point 3 of the Act of 17 February 2005 on the Computerisation of the Operations of Entities Performing Public Tasks (Journal of Laws 2024, item 1557, as amended), an information system is defined as a set of cooperating IT devices and software that enables the processing and storage of data, as well as the sending and receiving of data via telecommunications networks using an appropriate terminal device for the given type of network, within the meaning of telecommunications law. An identical definition appears in the Act of 18 July 2002 on the Provision of Services by Electronic Means.
It is accepted that an information system serves to process data, whereas a telecommunications system serves to transmit such data. Accordingly, a teleinformation system is an information system (in which computer data are processed) connected to a telecommunications network through which it can send and receive data. See: X. Konarski, *Commentary on the Act on the Provision of Services by Electronic Means*, Wolters Kluwer, Warsaw 2004, pp. 62–64; F. Radoniewicz, *Criminal Liability...*, pp. 282–284.

[6] In light of Article 2 point 35 of the Act of 16 July 2004 – Telecommunications Law (Journal of Laws 2024, item 34, as amended), a telecommunications network is defined as “transmission systems and switching or routing equipment, as well as other resources, including non-active network elements, which enable the sending, receiving, or transmission of signals by means of wires, radio waves, optical technologies, or other means using electromagnetic energy, regardless of their type.”

[7] This term is currently not defined in any legal act. A teleinformation network is a set of teleinformation systems—that is, information systems in which data are processed—connected to one another by telecommunications networks that enable the transmission of data between these systems. It is a broad structure, the emergence of which is linked to the process of convergence between information technology and telecommunications. See: X. Konarski, *Commentary on the Act...*, pp. 62–64; F. Radoniewicz, *Criminal Liability...*, p. 284; M. Świerczyński, in: J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Commentary on the Act of 18 July 2002 on the*

However, there is no doubt that these structures constitute the environment in which data are processed, stored, or transmitted[8].

Article 268a §1 of the Penal Code is formulated in an extremely imprecise manner. It reads: "whoever, without being authorized to do so, destroys, damages, deletes, alters, or hinders access to computer data." In legal doctrine, doubts have arisen (in my opinion, unfounded) regarding the object of the criminalized acts described as "destroying," "damaging," "deleting," and "altering." Is it—according to the literal wording—access to computer data (which is difficult to imagine in practice), or the computer data themselves? Clearly, the latter interpretation is the more logical one[9].

W. Wróbel and D. Zając point out another shortcoming of the provision in question. According to these commentators, the legislator does not clearly specify whether the object of the acts described in Article 268a of the Penal Code consists solely of computer data processed within an IT network (or computer system), or also data stored on memory media outside such a system—that is, on electronic data carriers such as CDs. They lean toward the view that Article 268a §1 protects all computer data that exist in a form enabling their operation and processing within an information system. In their opinion, the only data excluded from protection are those not in electronic form, i.e., "strings of characters that cannot be directly entered into an IT network (for example, data written on paper)."[10]. It seems that this position should—though with certain reservations—be accepted. The provision in question protects computer data processed within a computer or information system, as well as within a telecommunications network, and also data stored on electronic data carriers that do not constitute significant recorded information, since such information is protected under Article 268 §2 of the Penal Code[11], as a special provision, albeit one that provides the same penalty

---

Provision of Services by Electronic Means, Wolters Kluwer, Warsaw 2009, p. 39; A. Urbanek, in: J. Chustecki et al., *Teleinformatics Handbook*, IDG Publishing, Warsaw 1999, pp. 4–5.

[8] For a more extensive discussion of IT terminology relating to cybercrime and proposals for its clarification, see F. Radoniewicz, *Cybercrimes Against Computer Data and Information Systems in the Penal Code – Proposals for Reform*, C.H. Beck, Warsaw 2024, pp. 16–47.

[9] Similarly, W. Wróbel and D. Zając (in: *Penal Code*..., Commentary on Article 268a of the Penal Code, para. 8); conversely, B. Kunicka-Michalska (in: *System of Criminal Law*..., p. 1031); and A. Adamski, *Cybercrime – Legal Aspects*..., p. 59.

[10] W. Wróbel, D. Zając (in: *Penal Code*..., Commentary on Article 268a, para. 5).

[11] According to this provision, if the act specified in §1 (unauthorized destruction, damage, deletion, or alteration of a record of essential information, or otherwise preventing or significantly hindering an authorized person from

(imprisonment of up to three years). Therefore, Article 268 §2 should be abandoned, as Article 268a §1 can fulfill its function by providing protection against attacks on all computer data, whether stored on carriers or processed in information systems.

In conclusion, it should be emphasized that Article 268a §1 of the Penal Code can serve to criminalize actions involving the installation by an offender of, for example, a trojan, spyware, or software designed to take control of a targeted computer system in order to use it for a distributed denial-of-service (DDoS) attack. Such conduct clearly constitutes an unauthorized modification of computer data and thus an attack on their integrity[12].

In the second part of Article 268a §1, actions consisting of significantly disrupting (i.e., hindering the functioning of an information system) or preventing the processing, storage, or transmission of computer data are penalized. This wording refers to any activities affecting these processes that result in their improper operation or slowdown, as well as the distortion or modification of computer data being processed, transmitted, or stored[13]. The term "processing of computer data" is understood as performing logical operations on such data; "transmission" means sending data within an information system[14], and "storage" refers to keeping data within an information system. The latter two concepts are encompassed by the first. Automatic actions are those that occur wholly or partially without human intervention.

Article 268a §2 of the Penal Code provides a qualified type of the offence described in Article 268a §1. The qualifying element is the perpetrator's causing of substantial financial loss, with the applicable penalty being imprisonment from three months to five years.

---

accessing it) concerns a record on an electronic data carrier, the perpetrator is subject to a penalty of imprisonment for up to three years.

[12] See also A. Adamski, *The Council of Europe Convention on Cybercrime and the Issue of Its Ratification by Poland*, in: G. Szpor (ed.), *Internet. Protection of Freedom, Property and Security*, C.H. Beck, Warsaw 2011, p. 349.

[13] W. Wróbel, D. Zając (in: *Penal Code...*, Commentary on Article 268a, para. 10). See also P. Kardas, *Criminal-Law Protection of Information in Polish Criminal Law from the Perspective of Computer Offences. A Dogmatic and Structural Analysis in Light of the Current Legal Framework*, "Czasopismo Prawa Karnego i Nauk Penalnych" 2000/1, p. 96.

[14] P. Kozłowska-Kalisz takes a different view, arguing that the transmission of computer data should include both the electronic transmission of data and the transfer of a data carrier (see P. Kozłowska-Kalisz, in: *Penal Code...*, Commentary on Article 268a, para. 9). Similarly, J.W. Giezek (in: *Penal Code...*, Commentary on Article 268a, para. 10).

The essence of the offence known as IT sabotage, defined in Article 269 §1 of the Penal Code, consists of destroying, damaging, deleting, or altering computer data of particular importance for national defense, transportation safety, the functioning of government administration, other state bodies or institutions, or local government, or of disrupting or preventing the automatic processing, storage, or transmission of such data. According to Article 269 §2, the offence of IT sabotage may also involve destroying or replacing an electronic data carrier, or destroying or damaging a device used for the automatic processing, storage, or transmission of protected computer data. This offence carries a severe penalty—imprisonment from six months to eight years.

In creating Article 269 §1 of the Penal Code, the legislator likely intended it to serve as a tool for combating attacks of a logical nature. In contrast, Article 269 §2 was meant to protect computer data against physical attacks by criminalizing the destruction or replacement of an electronic data carrier (i.e., substituting it with another) or the destruction or damage of devices used for the automatic processing, storage, or transmission of computer data of particular importance. The consequences of such actions may include the physical annihilation of data (e.g., through the destruction of hard drives in a server) as well as hindering or preventing data processing (e.g., as a result of damaging network devices).

A behaviour that results in the destruction or replacement of a data carrier, or in the destruction or damage of a device used for processing, storing, or transmitting data, will not constitute the offence defined in Article 269 §2 of the Penal Code if, at the same time, the perpetrator did not destroy, damage, delete, or alter data of particular importance within the meaning of this provision, nor caused a disruption or prevention of the automatic processing, storage, or transmission of such data[15]. However, it should be assumed that if the perpetrator was aware of the purpose of the devices targeted by his actions, the behaviour should be classified as an attempt. The situation will be analogous when the perpetrator's act results only in damage to a data carrier (and not its destruction). If, however, the act simultaneously involves the modification or destruction

[15] Cf. W. Wróbel, D. Zając, *Penal Code...*, Commentary on Article 269, para. 10; A. Sakowicz, in: *Penal Code. Special Part*, ed. M. Królikowski, R. Zawłocki, vol. II, Commentary on Articles 222–316, Warsaw 2024, Legalis/el, Commentary on Article 269, para. 9.

of data of particular importance, it may constitute the offence described in §1[16]. Similarly, in the case of an attack on IT devices, damage that results in disruption of data transmission may be classified under Article 269 §1 of the Penal Code[17].

Under Article 269 §2 of the Penal Code, damage caused by the perpetrator to cables or wires used for transmission cannot be considered IT sabotage, as these cannot be regarded as devices. Such actions may, however, be classified as disrupting or preventing the automatic processing, storage, or transmission of computer data of particular importance—that is, as an offence under Article 269 §1[18]. From the above considerations, it follows that Article 269 §2 of the Penal Code is unnecessary[19].

Given the significantly greater importance of the information protected under Article 269 §1 of the Penal Code compared with the information protected under Article 268 §2, and the identical nature of the remaining elements of the offences criminalized by these provisions—combined with the difference in the severity of penalties and sanctions—the offence under Article 269 §1 is regarded as a qualified type in relation to the offence under Article 268 §2[20]. For these reasons, in my view, the same conclusion is justified with respect to the relationship between the offences under Articles 268a or 269a and Article 269 §1 of the Penal Code. In conclusion, I would like to draw attention to the issue of the incomplete implementation of Directive 2013/40 on attacks against information systems, which repealed Council Framework Decision 2005/222/JHA (hereinafter: Directive 2013/40)[21]. By requiring Member States to criminalize attacks involving unlawful interference with an information system (Article 4 of Directive 2013/40) and unlawful interference with computer data (Article 5 of Directive 2013/40), the Directive also provides for several aggravating circumstances in such cases. These include, among others, causing significant damage (Article 9(4)(b) of Directive 2013/40)

---

[16] Cf. A. Suchorzewska, *Legal Protection of Information Systems Against the Threat of Cyberterrorism*, Warsaw 2010, p. 227; W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 12; J. Znamierowski, *Criminal-Law Protection of State Functioning Against Computer Sabotage*, "Edukacja Prawnicza" 2014, No. 4, p. 24.

[17] Cf. W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 13.

[18] W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 15.

[19] Cf. F. Radoniewicz, *Criminal Liability...*, p. 325; cf. also W. Wróbel, D. Zając, in: *Penal Code...*, Commentary on Article 269, para. 9.

[20] P. Kardas, *Criminal-Law Protection...*, p. 96. See also A. Adamski, *Computer Criminal Law*, C.H. Beck, Warsaw 2000, p. 77; M. Kalitowski, in: M. Filar (ed.), *Penal Code. Commentary*, Warsaw 2012, p. 1211.

[21] OJ EU 2013 L 218/8.

or committing the offence against an information system that constitutes critical infrastructure (Article 9(4)(c) of Directive 2013/40). The occurrence of these circumstances should allow for the imposition of a penalty whose upper limit is at least five years of imprisonment[22]. Due to space limitations, I am forced to refrain from discussing this issue in the present study.

Article 269a of the Penal Code provides for criminal liability of a person who, without authorization, significantly disrupts the operation of an information system, teleinformation system, or teleinformation network through actions of a logical nature, such as the transmission, destruction, damage, or alteration of computer data. The protected interest is the security of the operation of the computer system and, consequently, the availability of the computer data processed within it.

An attack on the operation of an information system, teleinformation system, or teleinformation network is a logical, not a physical, attack—the disruption must be caused by the transmission, deletion, destruction, damage, or alteration of computer data. Examples include DDoS attacks.

Andrzej Adamski[23], Włodzimierz Wróbel and Dominik Zając[24] Andrzej Adamski and Włodzimierz Wróbel and Dominik Zając note that the provisions of Articles 268a and 269a of the Penal Code overlap in scope. The phrases "significantly disrupts or prevents the automatic processing, storage, or transmission of data" and "significantly disrupts the operation of an information system, teleinformation system, or teleinformation network" are essentially identical. The functioning of these systems and teleinformation networks is based precisely on the processing, storage, and transmission of data. Andrzej Adamski proposes that Article 268a of the Penal Code be treated as a tool for prosecuting offenders whose conduct does not fulfil the objective elements of Article 269a[25], while Włodzimierz Wróbel and Dominik Zając, on the other hand, propose applying Article 269a of the Penal Code in cases where there is a qualified disruption of the operation of a system or

[22] See F. Radoniewicz, *Cybercrime and the Law: An Analysis of Legal Governance in Europe*, Routledge, London 2025, pp. 125–137.
[23] A. Adamski, *Cybercrime – Legal Aspects*..., pp. 58–59.
[24] W. Wróbel, D. Zając, in: A. Zoll (ed.), *Penal Code*..., Commentary on Article 269a, para. 8.
[25] A. Adamski, D. Zając, *Cybercrime – Legal Aspects*..., p. 58.

network[26]. The offence under Article 269 §1 of the Penal Code should be regarded as the qualified type of the offence described in Article 269a. The current regulation of computer crimes that constitute attacks on the security of teleinformation systems requires a number of changes.

A significant shortcoming of the Polish regulation that must be pointed out is the overlap between the elements of the offence under Article 268a §1 of the Penal Code (violation of data integrity, hindering access to data, and disrupting their processing) and those of Article 269a (disruption of the operation of a computer system or teleinformation network). In my view, there are two possible ways to resolve this issue.

First, Article 269a could be removed, and Article 268a §1 amended accordingly to eliminate the ambiguities arising from the awkward wording of its first set of elements, for example by giving it the following wording: "whoever, without being authorized to do so, destroys, damages, deletes, alters computer data, or hinders or prevents access to such data." In this form, the provision would correspond to Articles 4 and 5 of the Convention on Cybercrime and Articles 5 and 6 of Directive 2013/40.

The second solution, proposed by Andrzej Adamski, is to limit the role of Article 268a to offences involving attacks on the integrity and availability of computer data, by giving it the following wording: "whoever, without being authorized to do so, destroys, damages, deletes, alters, or blocks computer data." In that case, Article 268a would correspond to Article 4 of the Convention on Cybercrime and Article 5 of Directive 2013/40, whereas Article 269a would correspond to Article 5 of the Convention on Cybercrime and Article 6 of Directive 2013/40[27]. In both variants, however, in my view, Article 268 §2 of the Penal Code should be abolished, as its function would be taken over by Article 268a §1. As mentioned earlier, Article 269 §2 is unnecessary, since its function could be fulfilled by Article 269 §1. The latter provision could then serve as the qualified type of the offence under Article 268a §1 (or under Article 268a §1 and Article 269a,

[26] W. Wróbel, in: A. Zoll (ed.), *Penal Code*..., Commentary on Article 269a, para. 8.
[27] A. Adamski, *Opinion on the draft act from parliamentary print no. 458: Government Draft Act Amending the Penal Code and Certain Other Acts*, http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf, pp. 10–11; accessed on 1 December 2025.

depending on which of the proposed modification variants were adopted).[28].[29] One should not forget the necessity of introducing higher penalties for perpetrators of attacks on critical infrastructure (as required by Directive 2013/40).

Conclusions

The analysis demonstrates that the current Polish criminal law provisions governing cyber-related offences are fragmented, partially overlapping, and in several respects insufficiently adapted to contemporary forms of cyberthreats. Article 268a suffers from significant imprecision and overlaps with Article 269a, which leads to interpretative inconsistencies and difficulty in distinguishing between attacks on data and attacks on system functionality. Article 269 §2 is largely redundant, as its protective function can be fulfilled through Article 269 §1. Likewise, Article 268 §2 appears unnecessary, given that Article 268a §1 could encompass the same scope of protection.

A coherent reform would require:

(1) clarifying the distinction between offences targeting data integrity and availability and those targeting the functioning of information systems;

(2) eliminating redundant provisions in order to create a more systematic and logically consistent structure of cybercrime regulations;

(3) adjusting penalties—especially for attacks on critical infrastructure—in accordance with the requirements of Directive 2013/40; and

(4) fully implementing the Directive's aggravating circumstances to ensure proper alignment of Polish law with EU standards.

Overall, the current legislation does not adequately address the complexity of modern cyberattacks, nor does it provide a streamlined and effective legal framework. Comprehensive legislative amendments are therefore necessary to improve clarity, coherence, and practical enforceability in the area of cybercrime.

---

[28] A similar solution was once proposed by A. Adamski, who argued that "certain elements of Article 268 §2 of the Penal Code should be removed, an equivalent of Article 5 of the Convention should be placed as the basic type of the offence of computer sabotage in §1 of Article 269 of the Penal Code, and the acts defined in §1 and §2 of the current Article 269 should be placed in the subsequent paragraphs of that article" (A. Adamski, *Government Draft for Adapting the Penal Code to the Council of Europe Convention on Cybercrime*. Paper presented at the Secure 2003 conference, http://www.cert.pl/PDF/secure2003/adamski.pdf, p. 6; the text is currently unavailable).

[29] F. Radoniewicz, *Criminal Liability*..., pp. 459–461.

References

Adamski, A. *Cybercrime – Legal and Criminological Aspects*. Studia Prawnicze 2005/4, pp. 51-76, 2005.

Adamski, A. "The Council of Europe Convention on Cybercrime and the Issue of Its Ratification by Poland." In: G. Szpor (ed.), *Internet: Protection of Freedom, Property and Security*. C.H. Beck, Warsaw 2011.

Adamski, A. *Opinion on the Draft Act from Parliamentary Print No. 458: Government Draft Act Amending the Penal Code and Certain Other Acts*. Available at: http://orka.sejm.gov.pl/RexDomk6.nsf/0/8C3096FB8C026D9AC12574720043B40C/$file/i1772_08-.rtf

Adamski, A. *Computer Criminal Law*. C.H. Beck, Warsaw 2000.

Adamski, A. *Government Draft for Adapting the Penal Code to the Council of Europe Convention on Cybercrime*. Paper presented at the Secure 2003 Conference.

Filar, M. (ed.). *Penal Code. Commentary*. Contribution by M. Kalitowski. Wolters Kluwer, Warsaw 2012.

Kardas, P. "Criminal-Law Protection of Information in Polish Criminal Law from the Perspective of Computer Offences." *Czasopismo Prawa Karnego i Nauk Penalnych*, 2000/1, pp. 25-120.

Kozłowska-Kalisz, P. In: M. Mozgawa (ed.), *Penal Code: Practical Commentary*. Wolters Kluwer, LEX/el. 2025.

Radoniewicz, F. *Cybercrime and the Law: An Analysis of Legal Governance in Europe*. Routledge, London 2025.

Radoniewicz, F. *Criminal Liability for Hacking and Other Offences Against Computer Data and Information Systems*. Wolters Kluwer, Warsaw 2016.

Sakowicz, A. In: M. Królikowski, R. Zawłocki (eds.), *Penal Code. Special Part, Vol. II: Commentary on Articles 222–316*. C.H. Beck, Warsaw 2024, Legalis/el.

Siwicki, M. *Cybercrime*. C.H. Beck, Warsaw 2013.

Giezek, J.W. In: J.W. Giezek (ed.), *Penal Code. Special Part. Commentary*. Wolters Kluwer, Warsaw 2021, Lex/el.

Konarski, X. *Commentary on the Act on the Provision of Services by Electronic Means*. Wolters Kluwer, Warsaw 2004.

Kunicka-Michalska, B. In: L. Gardocki (ed.), *System of Criminal Law, Vol. 8: Offences Against the State and Collective Interests*. C.H. Beck, Warsaw 2018.

Świerczyński, M. In: J. Gołaczyński, K. Kowalik-Bańczyk, A. Majchrowska, M. Świerczyński, *Commentary on the Act of 18 July 2002 on the Provision of Services by Electronic Means*. Wolters Kluwer, Warsaw 2009.

Urbanek, A. In: J. Chustecki et al., *Teleinformatics Handbook*. IDG Publishing, Warsaw 1999.

Wróbel, W., and Zając, D. In: W. Wróbel, A. Zoll (eds.), *Penal Code. Special Part. Vol. II, Part II: Commentary on Articles 212–277d*. Wolters Kluwer, Warsaw 2017. Commentary on Article 268a.

Znamierowski J., *Criminal-Law Protection of State Functioning Against Computer Sabotage,* "Edukacja Prawnicza" 2014, No. 4, p. 24-28.

„dot.pl" - czasopismo Rejestru domeny .pl

Governing Digital Ecosystems in the EU: A Coordinated Regulatory Approach[1]

Kitti Mezei
Hungarian Academy of Sciences, Centre for Social Sciences, Institue for Legal Studies, Hungary
ORCID: https://orcid.org/0000-0002-6497-1186
E-mail: mezei.kitti@tk.hu

Abstract

This paper analyses the EU's digital regulatory framework as a response to the ecosystem-based nature of digital markets, focusing on the GDPR, DSA, DMA, and AI Act. It argues that these instruments form a coordinated, human-centred regulatory model addressing market power, fundamental rights, transparency, and AI-related risks through ex ante obligations. While this approach strengthens legal coherence and global norm-setting, the paper also highlights concerns regarding regulatory rigidity, compliance burdens, and the EU's long-term technological competitiveness.

Keywords: transparency, risk-based regulation, DSA, AI Act, digital ecosystems

Received: 07.12.2025
Accepted: 19.12.2025
Published: 19.12.2025

Cite this article as:

K. Mezei, "*Governing Digital Ecosystems in the EU: A Coordinated Regulatory Approach*[1]"

DOT.PL, no. 1/ 2025, 10.60097/DOTPL/215839

Corresponding author:
Kitti Mezei, Hungarian Academy of Sciences, Centre for Social Sciences, Institue for Legal Studies, Hungary

E-mail: mezei.kitti@tk.hu

[1] The research was conducted with the support of the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

The foundations and objectives of the European Union's digital regulatory strategy

Several mutually reinforcing factors have prompted a rethinking of the European Union's (EU) digital legal regulations in recent years. New economic and social phenomena emerging as a result of technological developments – the market dominance of global online platforms, the explosive growth of the data economy[2] and the spread of artificial intelligence (AI) – have raised issues for which traditional legal frameworks did not provide adequate solutions.[3] However, the need for regulation did not arise solely from a market or competition law perspective; the need to enforce fundamental rights[4] also played a central role. Data protection, respect for privacy, security guarantees, and the protection of user rights are all factors that require increased attention in the digital space. In addition, there are political and economic motivations behind the creation of new legislation on digitalisation. These reflect the EU's efforts to strengthen the single market, as differing regulatory practices among Member States have hampered legal certainty and fair competition between businesses. At the same time, the promotion of technological autonomy and sovereignty[5] has emerged as a strategic goal, the essence of which is to reduce external technological dependence, primarily on the United States. For this reason, one of the EU's strategic objectives is to establish a *Digital Single Market,*[6] which aims to break down digital barriers between Member States and promote the smooth functioning of online services. The initiative aims to make it easier for both users and businesses to access digital goods and services, while providing a unified framework for the development of the digital economy, network security, and innovation support.

---

[2] For more details, see Matthew HINDMAN, *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy,* ORAC Publishing, Budapest, 2023.

[3] Bertin MARTENS: An Economic Perspective on Data and Platform Market Power. JRC (Joint Research Centre), European Commission, 2021.

[4] Giovanni DE GREGORIO, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society.* Cambridge University Press, 2022.

[5] Technological sovereignty has become one of the EU's central policy objectives and plays a decisive role in the EU's technological strategy, particularly in the regulation of AI. See Marton VARJU, 'Technology Sovereignty and AI Regulation in the EU: Regulatory Strategy and the Paradox of Choice', In: Marton VARJU – Kitti MEZEI (eds.): *The Challenges of Artificial Intelligence for Law in Europe*. 2025, pp. 65-84., and Luciano FLORIDI: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, Volume 33, Issue 3. 2020, 369–378.

[6] European Commission (2015): A Digital Single Market Strategy for Europe. COM(2015) 192 final.

This paper proceeds from the hypothesis that the European Union's recent digital legislation constitutes a coherent and coordinated regulatory response to the ecosystem-based structure of digital markets, rather than a collection of fragmented, sector-specific interventions. It assumes that the EU legislator has deliberately moved beyond traditional competition and sectoral regulation in order to address systemic risks arising from data-driven dominance, network effects, and the embedded use of AI within digital ecosystems. The primary objective of the paper is to analyse how the GDPR, DSA, DMA, and AI Act collectively shape the governance of digital ecosystems in the EU. More specifically, it aims (i) to conceptualise digital ecosystems as a regulatory object, (ii) to examine the common principles and regulatory techniques underpinning these instruments—particularly the human-centred and ex ante risk-based approach—and (iii) to assess the strengths and limitations of this coordinated regulatory model in light of innovation dynamics, compliance burdens, and global competitiveness.

Given the global nature of digitalisation, differences between national regulations would constitute an obstacle, which is why the EU has opted for regulation by means of directives in the field of digitalisation.[7] Unlike directives, regulations are directly applicable in Member States, thus ensuring legal certainty and the functioning of the single market. The best-known examples include the General Data Protection Regulation (GDPR),[8] the Digital Services Act (DSA),[9] the Digital Markets Act (DMA),[10] and the Artificial Intelligence Act (AI Act).[11] Together, these define the basic framework for the functioning of the digital space: they harmonise data protection rules, establish the responsibilities of online platforms,

[7] The literature describes this trend as the 'actification' of EU digital law, i.e. regulation taking the form of directly applicable regulations *('Acts')* instead of the previous directives. Vagelis PAPAKONSTANINOU – Paul DE HERT, *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis, and EU Law Brutality at Play.* Routledge, London–New York, 2024.

[8] Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[9] Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Digital Single Market and amending Directive 2000/31/EC (Digital Services Regulation).

[10] Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[11] Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, 168/2013/EU, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and amending Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Regulation on artificial intelligence)

and regulate the market behaviour of tech giants and the use of AI. Through regulation-level legislation, the EU not only strengthens the integrity of the internal market but also aims to develop a competitive and value-based regulatory model at the global level.

The EU's regulatory strategy aims to respond to the challenges posed by digitalisation and technological development by creating harmonised and uniform standards. As the primary instrument of EU legislation in this area is the regulation, the rules are directly applicable in the Member States. The regulatory concept focuses on European values and the protection of citizens, while promoting the process of digital transformation. Although one phase of this was already implemented in the period 2010-2020, the Digital Decade 2030 programme[12] sets out new objectives for the current decade: strategic gaps and high-risk dependencies must be addressed, supply and cybersecurity risks must be mitigated, and digital transformation must be facilitated. The programme also emphasises the regulation of data sharing and the protection of personal data in the context of new technologies. The EU's digital policy is therefore based on principles that are reflected in the regulations and take the form of specific obligations. These include, above all, a human-centred approach, which ensures that technological development prioritises the rights and interests of individuals over economic interests. The preamble to the AI Act explicitly states that the regulation of technology is based on the principle of 'human-centred and trustworthy AI'. The regulatory logic of the DSA and DMA is also in line with this: the protection of user rights, transparency, and security are also manifestations of this human-centred approach. Other key objectives include strengthening security, with a particular focus on cybersecurity and data protection, and developing sustainable digital ecosystems that promote economic growth in an environmentally and socially responsible manner. The aim of the EU's digital regulatory efforts is not to stifle innovation, but to encourage legislation to ensure that businesses use the latest technologies, such as AI, safely and transparently. One of the greatest added values of this regulatory approach is that it does not merely enforce economic and competition law considerations, but also places particular emphasis on risk management and the protection of fundamental rights. A uniform and clear legal framework contributes to strengthening trust between market

[12] Europe's digital future. https://www.consilium.europa.eu/hu/policies/a-digital-future-for-europe/

players and users and ensuring their safety, which in the long term promotes the sustainable development of innovation.

In addition, through the so-called *Brussels effect*,[13] the EU can act as a norm-setting power at the global level: regulations created for the internal market often function as international benchmarks, so the EU not only protects the interests of its own citizens, but also has a significant impact on the international development of digital technologies. At the same time, this regulatory solution also has its risks. One of the most significant problems is that rapidly obsolescent rules struggle to keep up with the dynamics of technological development, which can limit the flexibility of innovation. In addition, significant administrative burdens and compliance obligations can hit small and medium-sized enterprises particularly hard, putting them at a competitive disadvantage in global or even domestic markets. Finally, the geopolitical factor cannot be ignored: with the technological superiority of the United States and China, there is a risk that the EU will emerge as a regulatory power rather than a technological leader, which could lead to a decline in competitiveness in the longer term.[14]

Digital ecosystems

The common logic behind the EU's regulatory initiatives can be seen in the fact that they all reflect the specific functioning of digital ecosystems. In these systems, market and technological processes do not take place in separate sectors, but are closely intertwined and organised according to network logic. EU regulations therefore do not seek to address isolated problems, but rather to regulate a complex environment that is vividly illustrated by the operations of global technology companies. For example, the ecosystem-based strategies of Amazon, Google and Meta are simultaneously transforming the data economy, the ways in which AI is used and the structure of online platforms, clearly demonstrating that the challenges of digitalisation can only be addressed within a comprehensive and coordinated regulatory framework.

Although there is no uniform definition of the concept of a digital ecosystem, the literature typically starts from the analogy of a biological ecosystem: the interactions between

[13] This issue is discussed in detail in Anu BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

[14] Giovanni De GREGORIO, 'What is digital constitutionalism? A view from Europe', November 2022, https://www.ippi.org.il/digital-constitutionalism-in-europe/

participants, their interdependent roles and networked collaborations form an integrated system.[15] This model differs fundamentally from traditional business logic: the relationships between service providers, developers, users and devices create dynamic value based on network effects and data flows. It is no coincidence that key players in the global digital economy, such as Google and Meta, are basing their business strategies on this very model.[16] The EU's regulatory efforts are driven not only by the rapid spread of individual technologies, but also by their impact on market structures. Global technology companies not only have a significant market share, but have also established an ecosystem-based dominance in which their advantage stems not only from their current market share, but also from the fact that market and technological structures,[17] This dominance stems from the specific characteristics of ecosystem strategies: self-reinforcing network effects, asymmetric access to data and the functioning of algorithms create barriers to entry that competitors find difficult to overcome.[18]

[15] Sergey Yevgenievich BARYKIN et al., 'Economics of Digital Ecosystems', *Journal of Open Innovation: Technology, Market, and Complexity*, Vol. 6, No. 4, 2020, 3–4. https://doi.org/10.3390/joitmc6040124

[16] Jacques CRÉMER – Yves-Alexandre DE MONTJOYE – Heike SCHWEITZER, *Competition Policy for the Digital Era*, Report for the European Commission, 2019.

[17] Lina M. KHAN: *Amazon's Antitrust Paradox*. Yale Law Journal, Vol. 126, No. 3, 2017, 710–805. Khan points out that Amazon's dominance stems not only from its market share, but also from its ecosystem-based embeddedness, which provides self-sustaining advantages. This is also discussed by Martin KENNEY – John ZYSMAN: *The Platform Economy: Restructuring the Space of Capitalist Accumulation*. Cambridge Journal of Regions, Economy and Society, Vol. 13, No. 1, 2020, 55–76.

[18] CRÉMER – DE MONTJOYE – SCHWEITZER, ibidem. The report highlights the market dominance created by network effects, data monopolies and ecosystem integration, which are difficult to address with traditional competition law tools.

This position was confirmed by the General Court of the European Union in the case of Google LLC and Alphabet Inc. v European Commission (T-604/18), which held that the analysis of digital markets differs from traditional competition law logic. The judgment emphasises that classic parameters such as price or market share are less decisive in the digital economy, where innovation, access to data, network effects, user behaviour and multilateral platform characteristics are much more important factors (paragraph 115). The court explicitly states that these can also be interpreted as a digital 'ecosystem': thus, in the case of a digital ecosystem that brings together and encourages interaction between service providers, customers and several categories of consumers within a platform, the goods or services that form part of the relevant markets within that ecosystem may be complementary or interconnected due to their horizontal or vertical complementarity. When considered together, these relevant markets may also have a horizontal dimension, taking into account the system that brings their components together and any competitive constraints that exist within that system or stem from other systems (paragraph 116). Therefore, the relevant markets should not be examined in isolation, but in the context of the ecosystem, as the various elements of the platform may reinforce each other's impact. The judgment also points out that, when assessing Google's economic power, competitive pressures must be examined at several levels and from several angles, taking into account both the relationships within the internal ecosystem and the pressure from external systems (paragraph 117). The court therefore recognises that digital ecosystems are complex, intertwined structures in which market power does not stem solely from market share, but also from system-level interconnections and network effects (paragraph 118). Good examples of this are the dominant players in the market. Google's search engine is not only a market-leading service, but also part of an ecosystem, which includes advertising systems, Gmail, YouTube, Google Maps, the Android operating system, and newer AI solutions such as Gemini and DeepMind developments, that continuously strengthens its dominance in digital markets. Amazon's vertically integrated operations – as a marketplace, logistics network and cloud service provider – give it a complex advantage that is supported by its recommendation systems and AI-based assistant, Alexa, making

it difficult for its competitors to catch up. Meta (Facebook, Instagram, WhatsApp) is strengthening itself through user and data integration between social networks, while increasingly integrating generative AI – for example, in its content recommendation systems – thereby further deepening the market embeddedness of its ecosystem. This is another good example of how AI fits organically into the functioning of digital ecosystems, as it is one of the most important technological drivers today. It plays an essential role in data processing, the automation of decision-making processes and the personalisation of services. Global platform companies maintain their ecosystem-based dominance largely through these systems: their algorithms improve the user experience, amplify network effects, and facilitate the economic exploitation of data, reinforcing the 'winner-takes-most' dynamics characteristic of the platform economy.[19] AI is therefore not just a technological component, but a fundamental structural element within digital ecosystems. At the same time, this deep embedding poses significant regulatory risks: the opacity of algorithms, the risk of distortionary effects, the mass processing of personal data, and increasing market concentration all generate systemic problems.

The rise of large technology companies, therefore, raises fundamental regulatory issues. EU legislation has recognised that the concentrated market power of digital ecosystems can increase the vulnerability of users and consumers, that the opaque processing of personal data can violate fundamental rights, and that it can jeopardise fair competition for small and medium-sized enterprises. These problems justified the creation of a unified regulatory framework, the first milestone of which was the GDPR, which is also a model piece of legislation because it influenced the logic of subsequent digital regulations (DSA, DMA, AI Act). EU legislation therefore seeks to address the regulation of digital ecosystems within a unified framework, with normative solutions that ensure a human-centred approach, transparency and security, while supporting innovation and mitigating social, fundamental rights and competition risks. From a

[19] See Geoffrey G. Parker, Marshall W. VAN ALYSTYNE, and Sangeet Paul CHOUDARY, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*. New York, W.W. Norton, 2016, and Martin KENNEY and John ZYSMAN, The Platform Economy, Restructuring the Space of Capitalist Accumulation. *Cambridge Journal of Regions, Economy and Society*, 13 (1), 2020, pp. 55–76.

critical perspective, however, it is questionable whether these regulatory tools are capable of truly capturing and addressing the dynamic nature of digital ecosystems in the long term, or whether they offer fragmented and reactive responses.

EU legislative responses to digital ecosystems

The most important EU digital regulations – the GDPR, the DSA, the DMA and the AI Act – share several common features, suggesting that the legislator intends to create a coherent and coordinated regulatory ecosystem. Although at first glance these appear to be different areas of regulation, for online service providers operating or seeking to operate in digital ecosystems, these regulations together define the framework for lawful operation. It is therefore justified to examine the regulations not only individually but also in context, particularly in light of those solutions that specifically seek to shape the operation of these service providers. This approach is reinforced by the recognition, also emphasised in the literature, that digital markets have specific characteristics – such as network effects arising from ecosystem-based operation – to which the instruments of a single branch of law alone do not provide a satisfactory response. The EU has therefore ultimately opted for a regulatory model that applies multiple areas of law in a coordinated manner.[20]

Although these norms formally cover different areas, they are all based on the fundamental values of the EU, in particular a human-centred approach, the protection of fundamental rights and ensuring fair markets. Each of the key EU digital regulations has a specific impact on the protection of fundamental rights, for example. The GDPR explicitly builds on Articles 7 and 8 of the Charter of Fundamental Rights of the European Union to guarantee the right to privacy and the protection of personal data, including restrictions on automated decision-making (Article 22). The DSA primarily affects freedom of expression and the right to information by making content moderation and algorithmic ranking on platforms more transparent, while also ensuring users' rights to

[20] András PÜNKÖSTY: 'Where is European platform regulation headed? – An overview of the legal incentives for platform regulation and possible developments in merger control', In Bernát TÖRÖK – Zsolt ZŐDI (eds.): *The Age of Internet Platforms*. Ludovika University Press, Budapest, 2022. p. 175.

justification and redress.[21] The DMA contributes indirectly to the protection of fundamental rights: through its obligations on 'gatekeepers', it strengthens the rights to fair competition and consumer choice, promoting economic pluralism.[22] In contrast, the AI Act explicitly bases its regulatory logic on the protection of fundamental rights: it prohibits manipulative or discriminatory practices and sets strict requirements for high-risk AI systems. A central element of these requirements is transparency and ensuring the quality of training data sets, with the aim of avoiding discrimination and guaranteeing equal treatment.[23] In his monograph,[24] Zsolt Ződi already refers to platform law as a separate area of law. According to his interpretation, the DSA and other EU digital regulations (DMA, AI Act) do not simply aim to regulate the market, but create a new legal regime that is specifically tailored to the specific functioning of online platforms. This platform law as an independent discipline lies at the intersection of traditional areas of law (such as competition law, consumer protection, data protection, media regulation),[25] but also goes beyond them, as it addresses the risks arising from the functioning of digital ecosystems in an integrated framework.

One of the most important common points in EU regulation on digitalisation is the strengthening of transparency and reporting obligations. The DSA requires greater transparency in the functioning of algorithms, the DMA makes regular data reporting mandatory for gatekeepers, the GDPR emphasises detailed data processing information, while the AI Act requires, in particular, the 'explainability' and traceability of high-risk AI systems, as well as the preparation of detailed technical documentation

[21] According to the authors, the DSA is not merely a piece of technology regulation, but has digital 'constitutional' significance in the protection of fundamental rights: Natali Helberger – João Quaintas, The Digital Services Act and the Digital Constitution of Europe. *Journal of Media Law,* Vol. 13, No. 1, 2021. pp. 1–20.

[22] See Philipp HACKER – Johann CORDES – Janina ROCHON, Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond, *European Journal of Risk Regulation,* 2024/15(1), pp. 49–86.

[23] The recitals of the referenced regulations repeatedly refer to the protection of users, the protection of fundamental rights, transparency, and provisions aimed at reducing risks.

[24] Zsolt ZŐDI: *Platform Law.* Ludovika University Press, 2023.

[25] For more information, see Kelemen Bence KIS – Balázs HOHMANN, Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU, *Croatian Yearbook of European Law and Policy.* Vol. 19, No. 1. https://doi.org/10.3935/cyelp.19.2023.542 and Gergely GOSZTONYI – Ewa Galewska– Andrej Školkay, Challenges of Monitoring Obligations in the European Union's Digital Services Act. *ELTE Law Journal*. 2024/1. https://doi.org/10.54148/ELTELJ.2024.1.45, András TÓTH: European regulation of online platforms. *In Medias Res.* 2022/ 2., Klára GELLÉN, The modern business marketplace – Regulation of online platforms in the European Union. Economy and Law, 2020/11-12. pp. 16-19.

to facilitate auditing and *conformity assessment* procedures.[26]

Another common regulatory technique is the *ex ante* risk minimisation approach. Due to the dynamic nature of digital ecosystems, regulation cannot be satisfied with mere *ex post* sanctions, but imposes prior compliance obligations on service providers.[27] These include, for example, risk assessments, impact assessments and internal compliance mechanisms designed to prevent harmful effects.[28] This logic is similar to the regulatory philosophy of other high-risk sectors, such as financial or environmental law. This is not only a legal technique, but also aims to create a culture of compliance *(compliance by design)* in digital ecosystems.[29]

Concluding remarks

This paper examines the European Union's digital regulatory framework as a coordinated response to the ecosystem-based structure of contemporary digital markets. Focusing on the GDPR, DSA, DMA, and AI Act, it argues that EU digital regulation reflects a unified, human-centred approach that addresses market power, fundamental rights protection, transparency, and systemic AI-related risks through ex ante obligations. By conceptualising large platform operators as digital ecosystems rather than isolated market actors, the paper demonstrates why traditional competition and regulatory tools are insufficient and how EU law has adapted to network effects, data-driven dominance, and algorithmic governance. While the EU's model enhances legal coherence and positions the Union as a global norm-setter through the Brussels effect, the paper also highlights key challenges, including regulatory rigidity, compliance burdens—particularly for smaller firms—and potential long-term implications for European technological competitiveness.

---

[26] Martin HUSOVEC – Josef DREXL: Digital Services Act: Towards a More Transparent Digital Future? *Journal of European Consumer and Market Law*, Vol. 12, Issue 5, 2023, 190–197., and Michael Veale – Frederik ZUIDERVEEN BORGESIUS, Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 2021, pp. 97–112.

[27] Zsolt ZŐDI: The unsolvable dilemmas of platform regulation. In: Bernát TÖRÖK – Zsolt ZŐDI (eds.): *Digitalisation in society – Studies on the social and legal impacts of new technologies*. Budapest, Ludovika University Press, 2023. p. 81.

[28] Philipp HACKER – Justus ROCHON, Regulating High-Risk AI under the AI Act – Risk Regulation, Compliance and Liability. *European Journal of Risk Regulation*, 13(2), 2022, pp. 1–28. https://doi.org/10.1017/err.2022.7

[29] Klejda PRIFTI et al., Regulation by Design: Features, Practices, Limitations, and Governance Implications. Minds & Machines, Vol. 34, 2024/1, p. 13. https://doi.org/10.1007/s11023-024-09675-z.

In parallel with the consolidation of the EU's digital regulatory framework, increasing attention has been paid to proposals advocating partial 'deregulation' or regulatory simplification in the digital sector. These proposals are driven primarily by external pressure from the United States and by lobbying efforts of large technology companies,[30] which argue that the cumulative compliance burdens EU's digital legislation risk constraining innovation and undermining global competitiveness. From this perspective, EU digital regulation is portrayed as excessively rigid and insufficiently adaptable to rapid technological change, particularly in the field of AI.

Source of funding

The research was conducted with the support of the János Bolyai Research Scholarship of the Hungarian Academy of Sciences.

References

Matthew HINDMAN, *The Internet Trap: How the Digital Economy Builds Monopolies and Undermines Democracy,* ORAC Publishing, Budapest, 2023.

Bertin MARTENS: An Economic Perspective on Data and Platform Market Power. JRC (Joint Research Centre), European Commission, 2021.

Giovanni DE GREGORIO, *Digital Constitutionalism in Europe: Reframing Rights and Powers in the Algorithmic Society.* Cambridge University Press, 2022.

Marton VARJU, 'Technology Sovereignty and AI Regulation in the EU: Regulatory Strategy and the Paradox of Choice', In: Marton VARJU – Kitti MEZEI (eds.): *The Challenges of Artificial Intelligence for Law in Europe*. 2025, pp. 65-84., and Luciano FLORIDI: The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU. *Philosophy & Technology*, Volume 33, Issue 3. 2020, pp. 369–378.

European Commission (2015): A Digital Single Market Strategy for Europe. COM(2015) 192 final.

Vagelis PAPAKONSTANINOU, Paul DE HERT, *The Regulation of Digital Technologies in the EU: Act-ification, GDPR Mimesis, and EU Law Brutality at Play*. Routledge, London–New York, 2024.

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on the Digital Single Market and amending Directive 2000/31/EC (Digital Services Regulation).

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on competitive and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act).

[30] William ECHIKSON, 'Trump, tech and transatlantic Turbulence' *European view* Vol. 24. Issue 1. 2025.

Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, 168/2013/EU, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144, and amending Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Regulation on artificial intelligence)

Europe's digital future. https://www.consilium.europa.eu/hu/policies/a-digital-future-for-europe/

Anu BRADFORD, *The Brussels Effect: How the European Union Rules the World*, Oxford University Press, 2020.

Giovanni De GREGORIO, 'What is digital constitutionalism? A view from Europe', November 2022, https://www.ippi.org.il/digital-constitutionalism-in-europe/

Sergey Yevgenievich BARYKIN et al., 'Economics of Digital Ecosystems', *Journal of Open Innovation: Technology, Market, and Complexity*, Vol. 6, No. 4, 2020, pp. 3–4. https://doi.org/10.3390/joitmc6040124

Jacques CRÉMER, Yves-Alexandre DE MONTJOYE, Heike SCHWEITZER, *Competition Policy for the Digital Era*, Report for the European Commission, 2019.

Lina M. KHAN: *Amazon's Antitrust Paradox*. Yale Law Journal, Vol. 126, No. 3, 2017, pp. 710–805.

Martin KENNEY, John ZYSMAN: *The Platform Economy: Restructuring the Space of Capitalist Accumulation*. Cambridge Journal of Regions, Economy and Society, Vol. 13, No. 1, 2020, pp. 55–76.

Geoffrey G. Parker, Marshall W. VAN ALYSTYNE, Sangeet Paul CHOUDARY, *Platform Revolution: How Networked Markets Are Transforming the Economy and How to Make Them Work for You*. New York, W.W. Norton, 2016.

András PÜNKÖSTY: 'Where is European platform regulation headed? – An overview of the legal incentives for platform regulation and possible developments in merger control', In Bernát TÖRÖK – Zsolt ZŐDI (eds.): *The Age of Internet Platforms*. Ludovika University Press, Budapest, 2022. p. 175.

Natali Helberger – João Quaintas, The Digital Services Act and the Digital Constitution of Europe. *Journal of Media Law,* Vol. 13, No. 1, 2021. pp. 1–20.

Philipp HACKER – Johann CORDES – Janina ROCHON, Regulating Gatekeeper Artificial Intelligence and Data: Transparency, Access and Fairness under the Digital Markets Act, the General Data Protection Regulation and Beyond, *European Journal of Risk Regulation,* 2024/15(1), pp. 49–86.

Zsolt ZŐDI: *Platform Law.* Ludovika University Press, 2023.

Kelemen Bence KIS , Balázs HOHMANN, "Is There Anything New Under the Sun? A Glance at the Digital Services Act and the Digital Markets Act from the Perspective of Digitalisation in the EU", *Croatian Yearbook of European Law and Policy.* Vol. 19, No. 1. https://doi.org/10.3935/cyelp.19.2023.542

Gergely GOSZTONYI, Ewa Galewska, Andrej Školkay, "Challenges of Monitoring Obligations in the European Union's Digital Services Act.", *ELTE Law Journal.* 2024/1. https://doi.org/10.54148/ELTELJ.2024.1.45,

András TÓTH: European regulation of online platforms. *In Medias Res.* 2022/ 2.,

Klára GELLÉN, The modern business marketplace – Regulation of online platforms in the European Union. Economy and Law, 2020/11-12. pp. 16-19.

Martin HUSOVEC, Josef DREXL: Digital Services Act: Towards a More Transparent Digital Future? *Journal of European Consumer and Market Law*, Vol. 12, Issue 5, 2023, pp. 190–197.,

Michael Veale – Frederik ZUIDERVEEN BORGESIUS, Demystifying the Draft EU Artificial Intelligence Act – Analysing the good, the bad, and the unclear elements of the proposed approach. *Computer Law Review International*, 22(4), 2021, pp. 97–112.

Zsolt ZŐDI: The unsolvable dilemmas of platform regulation. In: Bernát TÖRÖK – Zsolt ZŐDI (eds.): *Digitalisation in society – Studies on the social and legal impacts of new technologies*. Budapest, Ludovika University Press, 2023. p. 81.

Philipp HACKER, Justus ROCHON, Regulating High-Risk AI under the AI Act – Risk Regulation, Compliance and Liability. *European Journal of Risk Regulation*, 13(2), 2022, pp. 1–28. https://doi.org/10.1017/err.2022.7

Klejda PRIFTI et al., Regulation by Design: Features, Practices, Limitations, and Governance Implications. Minds & Machines, Vol. 34, 2024/1, p. 13. https://doi.org/10.1007/s11023-024-09675-z

William ECHIKSON, 'Trump, tech and transatlantic Turbulence' *European view* Vol. 24. Issue 1. 2025

„dot.pl" - czasopismo Rejestru domeny .pl

Sztuczna inteligencja: od hakowania człowieka do hakowania natury

Kazimierz Krzysztofek

Uniwersytet SWPS (Emeritus), Wydział Nauk Społecznych Warszawa
ORCID: https://orcid.org/0000-0002-1772-8861
E-mail: kkrzysz1@swps.edu.pl

Niech przyroda podąża własną drogą. Ona rozumie lepiej swój interes niż my. (Michel de Montaigne)
Natura używa możliwie jak najmniej wszystkiego, żeby przetrwać. (Johannes Kepler)
Naturze nie powinno się rozkazywać, trzeba jej słuchać (Francis Bacon)

Słowa kluczowe: sztuczna inteligencja, hakowanie, systemy AI, Big Data

ESEJ

Received: 10.01.2025
Accepted: 13.01.2025
Published: 13.01.2025

Cite this article as:
K. Krzysztofek
"Sztuczna inteligencja: od hakowania człowieka do hakowania natury".

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/200061

Corresponding author:
Kazimierz Krzysztofek,
Uniwersytet SWPS, Wydział Nauk Społecznych
E-mail: kkrzysz1@swps.edu.pl

Świat w chmurze

Wraz z pojawieniem się hakerów weszło do słownika pojęcie „hakowania" przez które rozumiemy świadome ingerowanie w system komputerowy celem przejęcia nad nim kontroli i sterowania. Obecnie odnosimy to innych systemów, także przyrody.

„Hakując" przyrodę wydzieramy tajemnice jej, ale także sobie samym, ujawniamy nasze zachowania, mobilność przestrzenną. Sztuczna inteligencja (AI) uczyła się dotychczas przede wszystkim

od ludzi - danych, informacji, wiedzy, emocji itp., które rejestrujemy w wersji cyfrowej i którymi ją karmimy – m. in. wielkie modele językowe, wcześniej systemy eksperckie i mnóstwo innych „silników" sztucznej inteligencji.

Człowiek nigdy nie miał monopolu na emitowanie danych, bo to czyniła i czyni cała natura, żywa i nieożywiona. Nie miał też monopolu na ich postrzeganie, czy przetwarzanie. Miał natomiast monopol na ich interpretowanie, „ważenie", nadawanie im sensu, pozyskiwanie w ten sposób nowej wiedzy oraz integrowanie jej z już istniejącą.

W miarę rozwoju narzędzi rejestrujących rosło pozyskiwanie danych. Dzięki danym i ich obróbce, która oczyszczała „rudę danych" i nadawała im znaczenie oraz użyteczność, ludzie powiększali swoja wiedzę. Dzięki niej z kolei zdobywali coraz więcej danych, ponieważ mnożyły się źródła ich pozyskiwania nowym „szkiełkiem i okiem", o których wcześniej nie wiedzieli. Takim źródłem stawał się przekrój drzewa, który nic nie „mówił", dopóki nie było większej wiedzy o drzewach; nie wiedziano co „mówią" skały, dopóki nie wzrosła wiedza geologiczna. Wynalazki w sposób rewolucyjny rozwijały bazy danych o ludziach i przyrodzie, np. izotop węgla C14, który pozwolił datować relikty przeszłości miliony lat wstecz, wydzierać tajemnice nie tylko historii, ale także paleohistorii. Zatem im więcej informacji zintegrowanych z posiadaną już wiedzą i ją poszerzających, tym więcej się otwiera nowych źródeł sygnałów, które przestają milczeć i z których czytamy jak z otwartej księgi. Wiedza pozwoliła nam zdekodować kody informacyjne zawarte w tych źródłach.

Zadziałał *feedback* o cechach spirali kognitywnej i hermeneutycznej zarazem: prowadzi się coraz więcej badań, obserwacji przyrody, a także monitoringu ludzkich działań i zachowań, werbalnych niewerbalnych, dzięki czemu pozyskujemy więcej danych, przekształcanych w nową wiedzę. Ta wiedza jest wdrażana do praktyki, co wymusza zmiany, przyspieszenie procesów; rzeczywistość coraz bardziej się komplikuje. Trzeba więc znowu przyłożyć do tego jeszcze doskonalsze „mędrca szkiełko i oko" – badać, obliczać, przetwarzać, przekształcać w jeszcze nowszą, bardziej aktualną wiedzę i znowu zasilić nią praktykę społeczna, biznesową, polityczną, ekologiczną, klimatyczną itp.

Słowem, gromadzenie danych to czytanie świata z otwartej księgi, w której ciągle i dynamicznie przybywa stronic. Cywilizacja rosła dzięki tej spirali kognitywnej, która owocowała czujnikami, narzędziami do pomiarów itp.: detektor, sejsmograf, termometr, barometr, spirometr, stetoskop, spektrometr, mikroskop, luneta, okulary, skanery, ultrasonografia, kody kreskowe, kody QR, RFiD itp. W tle tego wszystkiego było przyspieszenie w zdobywaniu danych, ich przetwarzaniu i wdrażaniu w procesie podejmowania decyzji, a w końcu w produkcji dóbr i usługach.

Człowiek uzbrajał się w protezy - ekstensje zmysłów, które lepiej widziały, słyszały, czuły (dotyk, haptyczność), wąchały (detektory dymu). Mógł coraz lepiej postrzegać świat, organizmy żywe, przyrodę nieożywioną, wreszcie samego siebie, swój organizm, mózg. Istotne, że mógł to wszystko rejestrować, zwłaszcza zmiany, które są spostrzeżoną i uświadomioną różnicą.

Pozyskiwanie wiarygodnych danych jest kluczem do optymalnych decyzji i skutecznego zarządzania w skali kraju, gminy, miasta, firmy itp., nie ma bowiem dobrych decyzji w próżni informacyjnej, czy niedostatku danych. Wedle obiegowych opinii otacza nas morze danych, które poddane przetworzeniu wedle prawideł statystyki obliczeniowej pozwalają na prognozowanie, uchwycenie trendów, dzięki czemu, po przetworzeniu na decyzje, można rozwiązać sytuacje problemowe, uciec przed stanów krytycznych, a w najgorszym razie złagodzić skutki sytuacji katastrofalnej. Odgadnięcie trendu pozwala z kolei „wsiąść" na atraktor, wykorzystać nadzwyczajną szansę i zyskać przewagę nad konkurencją.

Jeśli prawa ludzkie i społeczne byłyby niezmienne jak prawa fizyki, jeśli człowiek byłby zewnątrzsterowny, jednowymiarowy, sterowany przez jeden algorytm, jeśli każdy byłby typowym egzemplarzem gatunku, funkcją itp., to wtedy byłoby możliwe odkrywanie takich praw. A i nauki społeczne byłyby wtedy naukami ścisłymi, opisywałyby zbiorowości ludzi tak jak fizyka opisuje atomy. Zdaniem A. Giddensa, tak się nie stanie, nauki społeczne nie są opóźnione względem ścisłych i przyrodniczych, a po prostu inne. W naukach przyrodniczych, przynajmniej w niektórych ich dziedzinach – zauważa – jest wiele przykładów twierdzeń, które zdają się spełniać warunek uniwersalności. W naukach

społecznych – ekonomii socjologii, psychologii i in. - nie ma żadnego twierdzenia dotyczącego zachowań ludzkich, indywidualnych i zbiorowych, które spełniałoby ten warunek.

Informacja to destylat danych potrzebny do podejmowania decyzji. Z perspektywy cybernetycznej natura jest systemem informacyjnym, który kreuje, emituje, dystrybuuje, odbiera i przetwarza dane. Dokonuje się w nim stale biologiczny (genetyczny, hormonalny, neuronalny) transfer informacji. Pozagenetyczny transfer dokonuje się w sferze przyrody nieożywionej.

Operuję pojęciem informacji rozumianej najprościej jako ustrukturyzowane strumienie danych, które rejestrowane przez nasze zmysły, są następnie przetworzone intelektualnie. To jest definicja niewystarczająca, ale trudno o w pełni satysfakcjonującą. Tyle jest definicji informacji, ile jest dyscyplin (różnie definiują informację statystyk, inżynier, psycholog, neurolog, dendrolog, socjolog itp.) Wspólne dla pojęcia „informacja" są takie elementy jak: niewartościująca treść komunikatu, zmiana otoczenia postrzegana przez podmiot (najprostsze rozstrzygnięcie miedzy „postrzegam – nie postrzegam"), wszystko co oddziaływa na nasze zmysły i co wpływa na orientację podmiotu wobec otoczenia. Karl Popper rozumiał informację, jako „przywołanie do świadomości", czyli przekształcenie nieuświadamianego w uświadamiane. przywołanie do świadomości czegoś, czego wcześniej ona nie rejestrowała. To jest jednak mało precyzyjne, poza świadomością dokonuje się bowiem olbrzymia ilość przepływów danych i ich przetwarzania.

Każda informacja, przefiltrowane dane, jest czyjaś, ponieważ jest rejestrowana przez aparat zmysłowy konkretnego podmiotu, który postrzega, wybiera, organizuje, nadaje znaczenie, przepuszcza przez własny filtr przeżyć, instynktu, emocji, rozumu, doświadczenia, wartościowania, intuicji, zdrowego rozsądku, własnej wiedzy, stereotypów, mądrości itp. W ten sposób informacja nabiera kształtu (staje się *in forma*), jest „odlewana" przez subiektywne ludzkie zainteresowania mające swe źródło w poznawczych i umysłowych procesach odbiorcy, często niepostrzeżenie przetwarzana i włączana w różne sektory pamięci o różnym stopniu dostępności i trwałości.

Big Data jako Piąty żywioł

Żyć w XXI wieku to znaczy żyć w cywilizacji zalanej potopem danych i informacji, są one jak hydrant, którego siła nas powala. Tak jak alkohol dane można wydestylować ze wszystkiego i przerobić je na użyteczne informacje, wiedzę. Tak sobie nieraz myślę, że przyjdzie taki dzień, kiedy mózg przestanie je chłonąć i trzeba będzie aplikować je dożylnie.

Temat danych obrósł tysiącami publikacji pokazujących ten fenomen naszego czasu z najróżniejszych pespektyw. Nie chcę wikłać się w szczegóły, lecz pokusić się o krótką refleksję, na ile ich inwazja w nasze życie znamionuje jakiś przełom cywilizacyjny, głęboką zmianę społeczną. Ludzie i organizacje, społeczności zawsze potrzebowały danych, bo bez nich nie ma informacji i nowej wiedzy. Informacje to dane przetworzone, wydestylowane, skontekstualizowane, zinterpretowane, zważone i jako takie są niezbędne w procesie optymalizacji decyzji. Ten zalew danych informacji istotnie jest. Ale czy dopiero dzisiaj? Przytoczę takie słowa: „Jedną z chorób obecnego stulecia jest nadmiar książek. Świat jest nimi tak obciążony, że nie sposób przetrawić obfitości jałowych treści, które rodzą się co dzień". Te słowa napisał Barnaby Rich, angielski pisarz. Ale wiecie Państwo kiedy? W 1613 r. Znaczyłoby to, że w każdej epoce ludzie mieli poczucie nadmiaru informacji i to nie tylko w zaawansowanych cywilizacjach. Nie płynęły one ze sztucznego środowiska, jakie stworzył człowiek, a z natury. Człowiek miał poczucie nadmiaru bo nie rozumiał otoczenia, w jakim żył, miał nikłą wiedzę o przyrodzie. Z czasem nabierał przekonania, że rozumie wszystko, a ten szczyt osiągnął w erze Oświecenia, gdy wyniósł *ratio* na piedestał. Zatem to przekonanie o wyjątkowości czasu, w jakim żyjemy wynika z niesprawiedliwej optyki historycznej, wydaje nam się, że żyjemy w najważniejszej epoce. Ale faktem jestem, że zalewa nas ten hydrant danych i informacji, bo stworzyliśmy technologie cyfrowe, które je generują i rozpowszechniają na skalę globalną.

Analizy frekwencyjne słów, jakimi posługujemy się w codziennej komunikacji, mediach, ekonomii i in. pokazują, że dane, często w wersji wielkie dane, albo wielkie złoża danych (Big Data), to słowo czy słowa, które stały się gwiazdami leksykalnymi. Kiedy mówimy o danych to natychmiast uruchamiamy wiele skojarzeń – przywołujemy do naszej świadomości pojęcia których nie było w obiegu kilkadziesiąt-kilkanaście-kilka lat temu. One są wskaźnikiem zmiany technologicznej, ale także społecznej i kulturowej:

bazy danych, sztuczna inteligencja, rozszerzona i wirtualna rzeczywistość, data science, chmura, metaverse 5G, w bliskiej przyszłości 6 G i cały nowy wokabularz słów z przedrostkami „i" i „e".

Wśród pojęć, które są kluczowe w analizach zmiany technologicznej na czoło wysuwają się właśnie dane, a zaraz po nich algorytmy, Są to pojęcia znane od dawna, ale w epoce cyfrowej nabierają one szczególnego znaczenia i nowego sensu. W potocznych narracjach jest wiele metafor danych: paliwo XXI w., waluta XXI wieku i in. Ilość i jakość usług w sieci i w realu zależna od ilości i jakości danych różnego typu o nas. Obok różnych wymiarów bezpieczeństwa bezpieczeństwo danych w odniesieniu do wielu aspektów naszego życia, zwłaszcza infrastruktury krytycznej urasta do najwyższej rangi.

Najczęściej rozróżniamy dane na osobowe i nieosobowe (pochodzące ze świata przyrody). Na przetwarzanie danych tylko w części dajemy zgodę, tam gdzie klikamy „zgadzam się", ale to tylko część, nie wyrażamy zgody na gromadzenie danych behawioralnych, np. płacenie kartą bankową a one są oczywiście pozyskiwane, przetwarzane i wykorzystywane w reklamie czy marketingu. Dane stały się środkami produkcji, bo Google, FB, Twitter nie oferowałyby swych usług za darmo. Korporacje chcą traktować wolny przepływ danych, jako przepływy kapitału. W Chinach funkcjonuje giełda handlu danymi, dzięki nim rozwijają one system kredytu społecznego. Coraz większej ilości danych potrzeba do funkcjonowania platform internetowych. Jako użytkownicy tych platform jesteśmy klientami, ale także towarami oraz źródłem surowców, bo przecież mówi się o danych surowych.

Bogate zasoby danych nie miałyby wielkiego znaczenia w gospodarce, administracji, ochronie zdrowia, itp. gdyby do ich przetwarzania nie zostały zaprzęgnięte algorytmy. Gromadzenie tak olbrzymiej ilości danych wieloaspektowych i ściśle ze sobą skorelowanych stwarza unikatowy cyfrowy ekosystem niezbędny do rozwijania sztucznej inteligencji i uczenia maszynowego, bo algorytmy się uczą na danych o ludziach. Bez nich człowiek by sobie z tym nowym bogactwem nie poradził. Dane są generowane w olbrzymim stopniu przez maszyny i one wyposażone w algorytmy je przetwarzają. Dzięki nim możliwe jest szybkie profilowanie, filtrowanie, predykcja, uczenie maszynowe i in.

Istotne jest pytanie, co wiemy o dzisiejszym kształcie społeczeństwa bogatego w dane w świetle najnowszych teorii. Na ile wcześniejsze teorie społeczeństwa informacyjnego wyjaśniają obecnie zachodzące procesy i czy w ogóle potrafimy je nazwać w adekwatnym języku. Teorie społeczeństwa powstawały już od lat 60. ub. wieku, rozwinęły się w latach 70. 80., ale wszystko to miało miejsce w czasie, gdy istniały tylko komputery jako wielkie machiny, a do lat 80. nie było komputerów osobistych (PC-tów i laptopów), Internetu w dzisiejszym kształcie (WWW) i nie było oczywiście BIG DATA. Dziś mamy Społeczeństwo hiperinformacyjne.

Nowy cykl cywilizacyjny

Spływają na nas ustrukturyzowane i nieustrukturyzowane strumienie danych, które rejestrowane przez nasze zmysły, są następnie przetworzone intelektualnie i wpuszczane w obieg społeczny za pośrednictwem różnorakich platform komunikacyjnych.

Nie ma relacji między ludźmi i ludzi z przedmiotami bez pozyskiwania danych, każdy z nas przekształca dane innych ludzi. Danych dostarcza całe *sensorium* człowieka. Są to w elementarnym rozumieniu postrzeżenia zmysłowe: obrazy, zapachy dźwięki, smaki, dotyk. Digitalizacja zmysłów pozwala na ich zapis w sztucznych systemach informacyjnych.

Człowiek nigdy nie miał monopolu na emitowanie danych, bo to czyniła i czyni cała natura, żywa i nieożywiona. Nie miał też monopolu na ich postrzeganie, czy przetwarzanie. Miał natomiast monopol na ich interpretowanie, „ważenie", nadawanie im sensu, pozyskiwanie w ten sposób nowej wiedzy oraz integrowanie jej z już istniejącą.

Jeszcze nie do końca sobie uświadamiamy społeczne konsekwencje zwrotu cyfrowego. Nie jesteśmy w stanie ogarnąć myślą, co oznacza to wchłanianie rzeczywistości cyfrowej przez społeczeństwo, gospodarkę, kulturę i inne sfery życia. Stwarza to niesamowite możliwości eksperymentowania, społecznego tworzenia rzeczywistości. Jest to forma rozpowszechniania wirtualnej koncepcji pieniądza, pracy i własności. Rozciągniecie obrotu na dobra cyfrowe znakomicie poszerza zakres usług i produktów. Większość z tych dóbr, to jeszcze cyfrowe kopie tych, które istnieją w realnej

rzeczywistości społecznej. Pojawia się jednak coraz więcej dóbr i usług, które są *digital native*, co podwaja, a w każdym razie zwiększa ofertę rynkową.

Każda informacja, przefiltrowane dane, jest czyjaś, ponieważ jest rejestrowana przez aparat zmysłowy konkretnego podmiotu, który postrzega, wybiera, organizuje, nadaje znaczenie, przepuszcza przez własny filtr przeżyć, instynktu, emocji, rozumu, doświadczenia, wartościowania, intuicji, zdrowego rozsądku, własnej wiedzy, stereotypów, mądrości itp. W ten sposób informacja nabiera kształtu (staje się *in forma*), jest „odlewana" przez subiektywne ludzkie zainteresowania mające swe źródło w poznawczych i umysłowych procesach odbiorcy, często niepostrzeżenie przetwarzana i włączana w różne sektory pamięci o różnym stopniu dostępności i trwałości

Oddychamy danymi. Dzięki nim lepiej widzimy świat, ale też świat cyfrowy nas lepiej „widzi". Człowiek epoki cyfrowej jawi się jako ogniwo *data flow*, terminal w przestrzeni przepływów by przywołać Manuela Castelssa. To, co robimy z danymi i co wielkie dane „robią" z nami to jeden z kluczowych dziś problemów cywilizacyjnych w każdym wymiarze: społecznym, politycznym, ekonomicznym, kulturowym i in.. Niezbędny jest stały monitoring, analiza doświadczenia i praktyk społecznych w niemal wszystkich orientacjach aktywności człowieka: ekspresywnej, ludycznej, kognitywnej, komunikacyjnej, normatywnej, narzędziowej i in., które manifestują się częściowo, a w wielu przypadkach także całościowo w środowisku cyfrowym. Jest to istotne zważywszy na istotne zmiany, jakie się dokonują w związku z przejściem od analogowości do cyfrowości.

Świat staje się systemem coraz bardziej złożonym, miliardy codziennych interakcji, transferów materialnych i symbolicznych produkują złoża danych, z których czerpiemy pełną garścią. Ten świat staje się układem coraz bardziej chaotycznym rodzącym zjawiska emergentne, które trudno przewidzieć, a często nawet nazwać w znanym nam języku. To znakomicie komplikuje jakiekolwiek prognozowanie.

Jak twierdzi Yuval Noah Harari staje się quasi religią. Zdanie się na inteligentne systemy analityczne i raporty, jakie one wytwarzają, niesie szanse ale i spore ryzyko. Należałoby zbadać, czy zaawansowana analityka nie grozi algorytmizowaniem ludzi, czy nie zdają się

oni na mądrość systemu; czy nie prowadzi do podświadomego niedoceniania własnej interpretacji i ewaluacji danych, bo „maszyna wie lepiej". Na takim psychologicznym gruncie może rodzić się bezkrytyczna postawa wobec systemów informacyjnych. Wybitni intelektualiści Stanisław Lem i Paul Virilio przestrzegali, że produkcja danych grozi tym, iż staną się one raczej śmietnikiem, wysypiskiem cyfrowym niż sezamem. Pętla danych zaciska się na szyi. Lem straszył „bombą megabitową"[1], a Virilio „bombą informacyjną"[2]. Ten drugi przywołuje Einsteina, który był przekonany, że wybuch tej bomby jest tylko kwestią czasu, w wyniku czego rozpęta się wojna informacyjna, oparta na globalnej interaktywności, a informacja zleje się z dezinformacją. W ciągu kilku lat wraz z „wynalazkiem" Big Data zmieniła się perspektywa: to już nie bomba, a nadzwyczajna szansa czerpania z nowego bogactwa.

Technologie pozyskiwania, przetwarzania i analizowania danych kreują nowe światy i nowych ludzi. Nie jesteśmy w stanie zdefiniować siebie bez nakreślenia obrazu naszego świata a zarazem nie możemy go opisać bez opisania, kim jesteśmy jako *digital humans*. Kiedy pojawia się nowa rzeczywistość, kiedy wkraczamy do nowego świata, to stajemy się nowymi ludźmi. Nowi ludzie w nowym świecie ciągle jeszcze nie bardzo wiedzą, jak się w nim poruszać, a nie mogą się dowiedzieć od starszych pokoleń, ponieważ one zostały ukształtowane w innej epoce.

Natura jako system informacyjny

Sztuczna inteligencja była zasilana wiedzą o przyrodzie pochodzącą od badaczy, którzy pozyskiwali dane o niej, przetwarzali je, destylowali, kontekstualizowali i w ten sposób aktualizowali istniejącą już wiedzę. **AI przestaje się uczyć tylko od ludzi**. Oczywiście potrafi się uczyć sama jak Alpha Go Zero, wcześniejsza wersja Alpha Go była jednak trenowana na historii szachów czy gry Go. Ale oto Amerykańska agencja ds.. zaawansowanych projektów badawczych na potrzeby Armii (DARPA) ogłosiła konkurs na „automatycznego naukowca". Mieści się to w ramach projektu ASKE (The Automating Scientific Knowledge Extraction, czasem uzupełnia się to o Modeling, ASKEM, zob.

[1] S. Lem, *Bomba megabitowa*, Kraków 1999.
[2] P. Virilio, *Bomba informacyjna*, Warszawa 2006.

Briscoe 2024)[3], co można przetłumaczyć jako automatyczne wydobywanie (ekstrakcję) wiedzy naukowej. Konkurs czeka jeszcze na rozstrzygnięcie. Jak czytamy w uzasadnieniu projektu świat – człowiek, społeczeństwo, przyroda stają się systemami coraz bardziej złożonymi. Rozstaliśmy się ze światem jako systemem prostym, a weszliśmy w nielinearny układ dynamiczny, czyli system złożony, który wytwarza zjawiska emergentne. A tych nie sposób przewidzieć, a jeśli już się pojawią, to nie potrafimy ich opisać na gruncie znanego języka i wyjaśnić na gruncie posiadanej wiedzy. System złożony może się składać z elementów, które w pojedynkę są proste, ale całość staje się złożona na skutek powiększającej się wykładniczo liczbie interakcji między nimi i potęgowemu rozkładowi relacji, jak to ma miejsce w sieci, na rynku, giełdzie, w pogodzie itp. Linearny przyrost interakcji w którymś momencie wywołuje przejście fazowe, co oznacza inną jakość. Molekuły wodoru i tlenu nie są mokre i przeźroczyste, a stają się (jako woda) takie po przekroczeniu pewnej skali i na tym właśnie polega emergencja. Fizycy nie wiedzą, jak do tego dochodzi.

Aparat poznawczy człowieka wyposażony w najbardziej zaawansowane technologie sam już sobie nie radzi z eksplorowaniem przyrody bez sztucznej inteligencji, która już nie tyle będzie go wspomagać, co **sama weźmie na siebie to zadanie**; zadanie dogłębnego zbadania nieliniowych układów dynamicznych: fizycznych, biologicznych, społecznych, hybrydowych i in. w celu ich modelowania i zwiększenia możliwości predykcyjnych, czyli obniżenia bariery postrzegalności nowych zjawisk różnej natury, aby zyskać dominację w świecie ludzi i przyrody. Od zarania człowieczeństwa toczyły się wojny o terytorium, które można nazwać wojnami 1.0. Wojny 2.0, to przede wszystkim wojny o dostęp do zasobów energii (surowce kopalne). W epoce komputera są to wojny 3.0 o supremację w mocach

[3] (ASKE) program aims to develop technology to automate some of the manual processes of scientific knowledge discovery, curation and application. ASKE is part of DARPA's Artificial Intelligence Exploration (AIE) program, a key component of the agency's broader AI investment strategy aimed at ensuring the United States maintains an advantage in this critical and rapidly accelerating technology area. ASKE seeks to develop approaches to make it easier for scientists to build, maintain and reason over rich models of complex systems – which could include physical, biological, social, engineered or hybrid systems – by interpreting and exposing scientific knowledge and assumptions in existing model code and documentation, identifying new data and information resources automatically, extracting useful information from these sources, integrating this useful information into machine-curated expert models, and executing these models in robust ways.

obliczeniowych. Na naszych oczach toczy się wojna o prymat w dziedzinie AI, w tym zwłaszcza o przejęcie kontroli nie tylko nad ludźmi, ale także nad przyrodą.

Dobrą intuicją wykazał się francuski filozof kultury, Jean Baudrillard (2001), który twierdzi, że nasza rzeczywistość, środowisko życia, środowisko naturalne zapośredniczone przez media, technologie, staje się coraz bardziej „obsceniczna" Jest obsceniczna dlatego, że technologie czynią ją bardziej widzialną niż rzeczywistość fizyczna postrzegana gołym okiem (nieuzbrojeni w protezy zmysłów percypujemy niewiele), wydzierają tajemnice ludziom, przyrodzie, światu. Nic się już przed nimi nie ukryje, ani priony, wirusy, jądra atomu, bakterie, czy kopulujące mszyce. Nakładka cyfrowa na ludzi, przyrodę, kosmos, dno oceanów, ujawnia potencjalnie wszystkie sekrety. Jest to coś w rodzaju uniwersalnego, przekraczającego wszystkie epoki WikiLeaks. Czy Wikileaks nie jest zgodny z duchem epoki?

Jak zmierzyć, zważyć, obliczyć świat, który zaczyna się „e"? Jest na to szansa, bowiem, jak prognozuje Arun Netravali, szef drugiej obok Media Lab w MIT największej wylęgarni innowacji, pokolenie dziś przychodzące na świat rozpocznie dorosłe życie w rzeczywistości, w której, inteligentne sieci otoczą planetę niczym żywa skóra. Czujniki rozmieszczone wszędzie będą przekazywać wszelkie informacje wprost do sieci – samomonitorującego się globalnego organizmu, jak nerwy transmitujące informacje do mózgu (Bomba, Krzysztofek 2011b). Ile jest w tym wszystkim wizjonerstwa, sztuki *fantasy*, a ile prognozy opartej na realnych przesłankach ekstrapolacji *lege artis*? Otóż nie jest to czysta fantazja, realnych przesłanek jest niemało.

Living Earth Simulator – Globalny Wikileaks?

Klucz leży w skonstruowaniu cyfrowego bliźniaka (*digital twin*) planety i najbliższych przestrzeni pozaziemskich, a w dalszej perspektywie kosmosu, którego eksplorację musimy powierzyć sztucznej inteligencji. Bez symulacji nie można sobie wyobrazić, nauki, badań, modelowania.

Oto badacze ze Szwajcarskiego Federalnego Instytutu Technologicznego budują od 2016 r. sieć superkomputerów do symulacji procesów i zjawisk dziejących się na Ziemi.

Inspiruje ich Wielki Zderzacz Hadronów funkcjonujący w laboratoriach CERN-a, który bada zachowania cząstek elementarnych. Nawiązując do metafory ze znanej książki Michela Houellebecqa ludzie to też cząstki elementarne, które się zderzają i pozostawiają ślady. Metaforą zderzacza posłużył się Jacob Helbing, inicjator założonego na dekadę projektu FuturICT", którego obecna faza nosi nazwę 'Living Earth Simulator". Jest to pomysł na to, co prognozował wspomniany Netravali: „system nerwowy Ziemi", który można nazwać planetarnym systemem operacyjnym. Wszystkie dane o tym, jak funkcjonują ludzie i przyroda będą po przetworzeniu mapą działań. Cel jest prosty: mieć większą wiedzę na temat tego, w którą stronę zmierza współczesny świat oraz co można zrobić, aby stymulować pożądane zmiany. Chodzi o odrobienie lekcji z niedawnej przeszłości: nie dać się zaskoczyć, przewidzieć trend, zwłaszcza taki, który grozi kryzysem. Czyli chodzi o system wczesnego ostrzegania, ale także ujawniania pozytywnych trendów, celem wzmocnienia szans. Inicjatorów projektu ożywia wiara w to, że „Symulator żywej Ziemi" pozwoli poradzić sobie z pęczniejącą masą danych o społeczeństwach i przyrodzie, aby socjologia, ekonomia, epidemiologia, i in. miały taki sam komfort jak fizyka i inne nauki ścisłe. Zagregowanie danych o ludziach w połączeniu z geofizyczną fotografią planety pozwoli na nową jakość – symulowanie bahawioru ludzkich społeczeństw wraz ich fizycznym środowiskiem, dzięki **sensoryzacji** („oczujnikowaniu"), „odronowaniu" planety i dzięki temu **rejestracji** niemal wszystkiego - ludzi, domów, miast, skał, chmur, oceanów, które znajdą się w jednej wszechogarniającej cyfrowej chmurze danych. Oznaczałoby to, że społeczeństwo, wszystkie sfery jego życia, da się umieścić w przyszłości w laboratorium cyfrowym, a wtedy przewidywanie stanie się być może mniej zawodne. Jesteśmy świadkami narodzin **cywilizacji samozapisu, samopokazu, autoanalizy i samoprzetwarzania natury**.

Idea Projektu ma się wyrażać w „zderzaniu" danych, informacji i wiedzy z różnych dziedzin. Projekt „Żywa Ziemia" to swoista nakładka cyfrowa na świat, zespół superkomputerów załadowanych bazami danych o ziemskim klimacie, populacji, gospodarce i przetwarzających te dane zgodnie z regułami fizyki – symulacji konfliktów, procesów ekonomicznych czy meteorologicznych. Przypomina to wiarę radzieckich planistów z lat 50. w to, że potężny komputer BESM-6 skonstruowany przez leningradzkich

matematyków nazywany wtedy mózgiem elektronowym pozwoli na pełną rejestrację i kontrolę wszystkich transakcji między jednostkami gospodarki uspołecznionej oraz drobiazgowe zaplanowanie zaopatrzenia ludności we wszystkie kategorie dóbr wedle doskonale rozpoznanych i zinwentaryzowanych potrzeb, m.in. typów rozmiarowzrostów człowieka radzieckiego.

To była utopia. Ale nie były pozbawione utopijnego pierwiastka zrodzone z rewolucji umysłowej i przemysłowej technokratyczne wizje świata zaplanowanego i zarządzanego nauką i techniką jak taśma produkcyjna. Niemiecki filozof, Peter Sloterdijk, któremu Kryształowy Pałac w londyńskim Hyde Parku wybudowany w połowie XIX w. na potrzeby wystawy światowej, wyposażony we wszystkie cuda ówczesnej techniki jawił się jako metafora, a zarazem utopia bezpiecznego świata, odpornego na kaprysy przyrody, nieprzewidywalność i ryzyko. Dziś ta utopia przyjmuje postać chmury danych. Wróciła nadzieja na powtórkę przewidywalnego, bezpiecznego świata w wersji „cyfrowego nieba".

Vilem Flusser przepowiadał to przed ponad trzema dekadami (Flusser, wyd. z 2011: 92). że w przyszłości społeczeństwa, jako całości, będą świadomie skierowane na tworzenie informacji i to będzie utrzymywać przy życiu całą naukę i kulturę. Poszedł jeszcze dalej niż Manuel Castells i cała plejada badaczy rozwijających jego myśl - zaproponował pojęcie, które doskonale oddaje ducha naszego czasu w trzeciej dekadzie obecnego stulecia. To pojęcie to programatyzm. Programu nie wymyślił człowiek – wymyśliła go natura. Dla Flussera wszystko jest programem: ewolucja, funkcjonowanie organizmów, łańcuchów aminokwasów, zapłodnienie, nawet wszechświat jako taki. Ten „imperializm" programu dobrze odzwierciedlił Jorge Luis Borges w swej prognozie biblioteki przyszłości „Babel", w której znajdą się wszystkie napisane przez wszechpotężny program komputera (zapewne będzie to superkomputer kwantowy) książki, zdolny do stworzenia wszystkich możliwych kombinacji tekstów kultury z istniejących kodów, znaków, obrazów dźwięków i in..

W ten sposób narodziła się metoda postrzegania świata o cechach informacyjnego redukcjonizmu. Wszystko można było postrzegać przez pryzmat sytemu informacyjnego, człowieka i inne organizmy, procesy życiowe, praca mózgu, systemu nerwowego, cały proces ewolucji jako program, który zapewnia ład i chroni przed entropią.

Co w istocie oznacza „zautomatyzowane wydobywanie wiedzy naukowej" anonsowane przez projekt ASKE. To rozpoczyna **nowy cykl cywilizacyjny**. Można powiedzieć *dejà vu*: obok „kopalin analogowych" przetwarzanych następnie przemysłowo, wydobywa się dziś „kopaliny cyfrowe" (*data mining*). Mamy zatem do czynienia jakby z powtórzeniem cyklu wydobywczego i przemysłowego. Można w tej analogii pójść o krok dalej: tak jak skończyła się na wielką skalę faza zbieractwa i myślistwa i ludzie przeszli na hodowlę, tak myślistwo i „polowanie na dane" zostało w dużym stopniu zastąpione przez „uprawę danych" (*data farming*), coraz bardziej zalgorytmizowaną i zautomatyzowaną. Nakładka AI na rzeczywistość (maszyny widzenia, słyszenia, rejestrowania itp.) znacznie ją poszerza pod względem percepcji: rzeczywistość wirtualna, wszędobylski computing, rzeczywistość rozszerzona, inteligencja tła, przetwarzanie w chmurze i inne. Wszystkie dotychczasowe fazy cyklu były dziełem człowieka. Początek nowego cyklu miałby oznaczać przejęcie kontroli nad eksploracją świat przez systemy autonomicznej sztucznej inteligencji.

Człowiek nigdy nie miał monopolu na emitowanie danych, bo to czyniła i czyni cała natura, żywa i nieożywiona. Nie miał też monopolu na ich postrzeganie, czy przetwarzanie. Miał natomiast monopol na ich interpretowanie, „ważenie", nadawanie im sensu, pozyskiwanie w ten sposób nowej wiedzy oraz integrowanie jej z już istniejącą. Dziś „...narzędzia wspomagające zmysły zyskały nowe możliwości. Powstały maszyny do widzenia, zdolne utrwalać doświadczenie wedle swych matryc czasu i przestrzeni. Niektóre z nich przejmują nawet obowiązek patrzenia uprzednio ciążący na użytkowniku. Dzięki optyce cyfrowo-falowej patrzenie nie jest już potrzebne, by widzieć. Powstały maszyny poznania, które są władne wytwarzać i widzenie i obrazy, w tym obrazy trójwymiarowe, pachnące i mobilne" (Banaszkiewicz 2011)

Oznaczałoby to, że wielki postęp dokona się już nie przez naśladowanie ludzkiej inteligencji i przetwarzaniu wiedzy człowieka o przyrodzie, a **na odkrywaniu inteligencji samej natury,** nie ulega bowiem wątpliwości, że to ona, choć bez własnej świadomości (ale tego do końca nie wiemy) zapewnia przyrodzie ład i harmonię. Nie wiemy jeszcze czy jesteśmy już w fazie przejścia od wąskiej AI do AGI (*artificial general intelligence*), a w dalszej perspektywie SuperAI oznaczającej nadejście osobliwości (*singularity*), jak wieszczy wizjoner Ray Kurzweil.

Na horyzoncie pojawia się Q* (Qstar) – nowa generacja AI, która „zhakuje" matematykę, co by oznaczało, że wejdzie ona w rolę fizyków, astrofizyków, chemików, biologów, biomedyków i innych przedstawicieli twardych nauk – *scientists*, dla których matematyka jest królową wszystkiego. Być może wtedy powstanie tak wytęskniona ogólna teoria wszystkiego, o czym marzy Stephen Wolfram (2002). Wszystkie tajemnice natury zostaną rozwikłane. Kosmos będzie widać jak na dłoni. Człowiek zawsze wydzierał tajemnice naturze, ale w tym wydzieraniu zastąpi go sztuczna inteligencja nowej generacji. AI będzie odkrywać prawa przyrody, korelować dane o niej w nieznany dla ludzkiej inteligencji sposób. A kiedy je odkryje to będzie robić z nich użytek, np. syntetyzować nowe leki, czego „ludzka" medycyna nigdy by nie potrafiła. Tak jak nie potrafiła odkryć więcej niż 200 białek, a AI odkryła ich ponad 5 mln.

To już ekstensja i augmentacja zmysłów człowieka za pomocą narzędzi, a własny aparat poznaczy przyrody, imitacja już nie tylko inteligencji człowieka, ale także inteligencji przyrody.

Wedle Jamesa Ralpha Benigera (1986) obieg informacyjny istniał w ziemskim ekosystemie od zawsze, chociażby pod postacią biokodowania DNA, którego błędy często reorientowały tory ewolucji. Ale nauczyliśmy się go odkrywać stosunkowo niedawno. Równolegle uczymy się kontrolować zjawiska (społeczne, ekologiczne, gospodarcze) za jego pomocą i jest to miara postępu społecznego. Im więcej informacji, tym więcej analizy i kontroli owej informacji oraz kontroli za pomocą tejże informacji. Poszukiwanie skutecznych środków kontroli staje się kwestią przetrwania w złożonym środowisku informacyjnym, zwłaszcza w sytuacji, gdy wartość informacji w wielu urządzeniach np. samochodu autonomicznego), wartość software'u, a także wiedzy, umiejętności, kompetencji koniecznych do ich zaprojektowania, przekracza wartość materiału, z którego zostały wytworzone oraz energii niezbędnej do ich produkcji i wprawienia w ruch w reżymie automatyzacji i autonomizacji.

Z ustaleń Castellsa i Benigera wynika, że w epoce cyfrowej górę bierze rozumienie informacji jako elementu organizacji systemów wszelkiego rodzaju. Dla Alberta-Lászlo Barabásiego (2002) dane transformowane w informacje mają służyć kontroli systemów w

celu predykcji ich zachowań, czyli obniżeniu bariery postrzegalności nowych trendów, które mogą zmienić warunki funkcjonowania planety, społeczeństwa czy biznesu. Jest więc olbrzymia jest pokusa, aby maksymalizować pozyskiwanie danych, co stwarza szanse śledzenia trendów i domyślania się przyszłości, a tym samym zmniejszania niepewności.

Człowiek od zarania cywilizacji i kultury tworzył artefakty poszerzając w ten sposób obszar artyficjalizacji (usztuczniania) środowiska życia. Mimo to wolumen danych i informacji, jakie produkuje, to drobna cząstka tego co wytwarza przyroda, a co AI nowej generacji przetwarza w wiedzę bez udziału człowieka. Pomocne w tym są *Large Action Models* (LAM, wielkie modele działania), które się różnią od LLM – wielkich modeli językowych. Te drugie dzięki promptowaniu tworzą różnego rodzaju kreatywny kontent, ale nie są w stanie same podejmować działań w realnym świecie, *actions models* to potrafią, nawet przeprowadzać eksperymenty naukowe. Łączą w sobie zdolności modeli językowych ze zdolnościami performatywnymi. Stąd przekonanie niektórych badaczy, że mamy do czynienia z *pivotal advancement in artificial intelligence* (Takyar 2023). Jeśli odniesiemy to do przyrody to w niektórych wizjach wiedza o niej tworzona przez ludzkie umysły będzie uboższa od tej kreowanej przez „automatycznego naukowca", który się będzie uczył na danych pozyskiwanych przez samego siebie z oczujnikowanej planety (adaptory, sensory, transmitery, efektory, mikronawigatory, aktuatory, bikony, tagi RFID i in.), które monitorują i rejestrują działanie głównych sił przyrody: elektryczności, tektoniki (m. in. tsunami) ruchów powietrza (wiatry, huragany, tornada i ich efekty – fale morskie), wyporu, tarcia, grawitacji, mocnego i słabego promieniowania, magnetyzmu, sił jądrowych. „Automatyczny naukowiec" będzie przetwarzał te dane w sobie tylko znany sposób, w niewidocznej „czarnej skrzynce".

Nadzieje pokłada się w tym, że sztuczna inteligencja pozwoli na automatyczne zarządzanie środowiskiem w schyłkowej epoce Holocenu i rodzącej się epoce Antropocenu – nowej warstwy geologicznej tworzonej już nie przez naturę a człowieka, cywilizację i cztery główne jej tworzywa: stal, cement, amoniak, węglowodory (plastik). Widać tę nową warstwę np. w postaci tysięcy ton odpadów plastikowych zalegających w glebie czy dryfujacych wysp na oceanach).

Ta epoka jawi się naukowcom jako epoka postnaturalna. Bradley Cantrell i Laura J. Martin proponują delegowanie zarządzania środowiskiem naturalnym systemom sztucznej inteligencji (Cantrel, Martin 2017). „Zadaniem sztucznej inteligencji byłoby podtrzymywanie autonomii nie-ludzkich procesów ekologicznych, która w tym zakresie miałaby zastąpić bezpośrednią interwencję człowieka" (Knosala 2023: 135). Chodzi o przewidzenie zachowań postnaturalnych, antropogenicznych wynikających z działalności człowieka. Wiedza o tym pozwoli na orientację, w czym człowiek zawinił i co ma zrobić, żeby zminimalizować skutki swoich działań, a także obniżyć barierę postrzegalności niezawinionych zjawisk przyrodniczych.

Problemem staje się znalezienie sposobów translacji danych z czujników na język przyjazny ludzkiej percepcji, istnieje bowiem wielka luka między danymi od nich pochodzącymi a ludzkimi, naturalnymi postrzeżeniami zmysłowymi (Krzysztofek 2012). Wielu rzeczy nie doświadczamy już własnymi zmysłami, one są ograniczone, ponieważ nie kwantyfikują danych w jednostkach wagi, odległości, wilgotności, temperatury: widząc, ważąc, słysząc, dotykając mierzymy tylko „na oko". Zwierzęta mają o wiele bardziej wyostrzone zmysły, ale człowiek ma protezy zmysłów, dzięki którym może wszystko obliczać – miary, wagi, ilości. Niedoskonałość narządów rekompensują przyrządy, które dzięki AR kwantyfikują fizyczność (Dublon, Paradiso 2014).

Jak będzie w przyszłości? „Nie można całkowicie wykluczyć takiego rozwoju metod i narzędzi matematycznej analizy nieliniowej, dzięki którym możliwe stanie się opisanie przy pomocy funkcji i równań całej złożonej rzeczywistości biologicznej, psychologicznej i społecznej, i to z uwzględnieniem ich dynamiki, rozwoju i zdolności do transgresji. Można jednak sądzić, że nawet gdyby udało się to kiedyś osiągnąć, to uzyskany wzór na życie biologiczne, życie psychiczne lub życie społeczne, pozostałby wysoce abstrakcyjnym zapisem, którego wartość praktyczna nie wykraczałaby poza możliwości dokonywania komputerowych symulacji, ukazujących... chaotyczność i losowość tego, co owym *wzorem* zostało zapisane" (Łuczak 2012: 7).

AI kreuje nowy typ relacji i interakcji między człowiekiem i narzędziem poznawania otoczenia, tak jak go opisał amerykański filozof nauki i technologii, Don Ihde. Pierwszy typ to **narzędzia na zewnątrz człowieka**, jak np. kij czy młotek, czy bardziej zaawansowane

jak np. termometr za oknem. Drugi typ to **narzędzia i technologie wchodzące do wnętrza człowieka** (jak rozrusznik serca, nanoboty), albo będące symbiotyczną ekstensją jego organów czy zmysłów (protezy kończyn, okulary, lunety), bionika (połączenie biologii i techniki). Typ trzeci to **technologie tła**, wysoce zaawansowane inżynieryjnie będące wytworem rewolucji przemysłowej (elektryczność, której nie widzimy, urządzenia AGD). Typ czwarty to **ekstensje umysłu epoki informatycznej** w postaci komputera, smartfona, czy obecnie sztucznej inteligencji. Ich cechą jest to, że *software* emigruje z umysłu na zewnętrzne nośniki. W tym typie relacji technologie nie są już w tle; one, dotyczy to zwłaszcza AI, stają się niejako partnerem komunikacyjnym, interaktorem, już nie przedmiotem, a INNYM. Ewolucja wyposażyła nas w narzędzia do interakcji z innym człowiekiem i tak skłonni jesteśmy traktować AI.

Konkluzje

Rozwój sztucznej inteligencji był budowany na emulowaniu ludzkiej, choć porównywanie jej w skali 1 do 1 nie ma sensu (gdy np. mówimy, że jest ona dziś na poziomie ośmioletniego dziecka). To jest porównywanie jabłek do bananów.

Hakowanie w potocznym rozumieniu to, jak powiedziano, przejęcie nad czymś kontroli i sterowania. We wszystkich fazach rozwoju od Neolitu, Mezolitu, industrializmu po informacjonizm człowiek sam hakował naturę przez pomocy coraz bardziej zaawansowanych narzędzi, wiedza i orientacja instrumentalna wychodziły „z głowy" do samych narzędzi, nad którymi jednak człowiek miał kontrolę, aż doszedł do etapu, gdy narzędzie się zautonomizowało (AI) i samo zaczęło hakować nie tylko człowieka, ale także naturę.

Eksploracja przyrody to także eksploracja człowieka, jego struktury psychosomatycznej, może lepiej się uda, bo umysł człowieka nie został stworzony by eksplorować samego siebie, gdy podmiot eksploruje sam siebie jako przedmiot. Jaka będzie rola człowieka? Nadal dostęp do danych musi się dokonywać za pośrednictwem ludzi, którzy oczujnikowywują planetę. Na razie mamy do czynienia z automatyzacją *researchu*. Istnieje program komputerowy AI Scientist, który działa jako naukowy asystent, stażysta,

ale w przyszłości automatyczny naukowiec będzie sam tworzył teorie naukowe, bez udziału ludzi, będzie sam generował dane.

Mamy tu do czynienia z jakimś cyklem: przed epoką Oświecenia ludzie czuli się we władzy sił nadprzyrodzonych. Oświecenie dało im poczucie władzy nad przyrodą, wiarę w rozum a władzę na tym padole sami sobie wybierali i na nią zrzucali odium za nieudolność. W wieku AI, której nie rozumiemy, mamy doń nabożny stosunek i skłonni jesteśmy ją traktować jako nowe bóstwo i godzić się na kontrolę nad nami. Słowem, tak jak przed wiekami ludzie nie mieli poczucia władzy nad przyrodą, dziś nie maja poczucia władzy nad technologią. Można jednak mieć nadzieję, że w miarę upowszechnienia wynalazek ten spowszednieje, ulegnie banalizacji nie będziemy się zastanawiać, jaki „diabeł w nim siedzi".

Bibliografia

Banaszkiewicz, Karina (2011) Audiowizualność i mimetyki przestrzeni, Oficyna Naukowa: Warszawa 2011

Baudrillard, Jean. 2001. Przed końcem, rozmawia Phillipe Petit. SIC! Warszawa

Briscoe, Erika. 2024. Automating Scientific Knowledge Extraction and Modeling (ASKEM) https://www.darpa.mil/program/automating-scientific-knowledge-extraction-and-modeling (dostęp 20.05. 2024)

Cantrell, Bradley, Laura Martin, and Erle Ellis. 2017. Designing Autonomy: Opportunities for New Wildness in the Anthropocene. Trends in Ecology & Evolution 32, no. 3 (2017):156–66.

Dublon Gershon, Paradiso. Joseph A. 2012. Extra Sensory Perception. Scientific American 311(1):36-41 311(1):36-4

Kelly, Kevin. 2007. The Technium and the 7Th Kingdom of Life http://www.edge.org/3rd_culture/kelly07/kelly07_index.html (dostęp 15. 06. 2024)

Knosala. Bartłomiej. 2023. Zarządzanie środowiskiem naturalnym przez sztuczną inteligencję. Ograniczenia i wyzwania narracji postnatury, „Ethos" Tom 36, nr 4 2023

Krzysztofek. Kazimierz. 2012. – BIG DATA SOCIETY. Technologie samozapisu i samopokazu: ku humanistyce cyfrowej. http://www.kulturaihistoria.umcs.lublin.pl/pl/archives/3626

Łuczak, Mikołaj. 2016. Przestrzenie komunikacji społecznej. Akademia Pomorska w Słupsku. Słupsk

Mazurkiewicz. Piotr. 2024. Tajemniczy Q*, https://cyfrowa.rp.pl/globalne-interesy/art39456031-tajemniczy-q-sam-altman-odkryl-w-openai-cos-co-moze-zagrozic-ludzkosci, dostęp 24.06. 2024

Szpunar, M. 2012. Nowe–stare medium Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego. IFIS PAN. ISBN 987-83-7683-061-2

Szpunar, M. (2021). Internet spłyca myślenie. In: S. Iwasiów (Ed.). Po szkole: rozmowy o edukacji (2015-2020). Uniwersytet Szczeciński, 240–251. *ISBN*-13, 978-83-7972-450-

Takyar, Akash (2023) Actionable AI: An evolution from Large Language Models to Large Action Models, https://www.leewayhertz.com/actionable-ai-large-action-models/, dostęp: 26.06.2024

Wolfram, Stephen. 2002. A New Kind of Science, Wolfram Media, Champaign, Il

„dot.pl" - czasopismo Rejestru domeny .pl

Online Conspiracy Theories and the Role of Conspiracy Influencers

Stefano Lovi
University of International Studies of Rome – UNINT, Italy
ORCID: https://orcid.org/0009-0009-9978-8689
E-mail: stefano.lovi@unint.eu

Received: 03.04.2025
Accepted: 26.05.2024
Published: 26.05.2024

Cite this article as:
S. Lovi, "Conspiracy Theories and the Role of Conspiracy Influencers"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/205575

Corresponding author:
Stefano Lovi, University of International Studies of Rome UNINT, Italy
E-mail: stefano.lovi@unint.eu

Abstract

The proliferation of online conspiracy theories has significantly increased with the advent of social media, transforming niche beliefs into mainstream discussions. Conspiracy influencers play a pivotal role in amplifying these theories, leveraging platforms like YouTube, Instagram, and Telegram to disseminate unverified narratives to a wide audience. This phenomenon intertwines sociological, psychological, and media aspects, reflecting a crisis of trust in public institutions. Cognitive biases such as confirmation bias and apophenia facilitate the acceptance of conspiratorial ideas, while digital environments like echo chambers and filter bubbles reinforce these beliefs. The role of conspiracy influencers, such as Cesare Sacchetti, highlights how charismatic personalities exploit the information vulnerabilities of their followers, spreading disinformation under the guise of truth. Countering conspiracy theories requires comprehensive strategies,

including digital literacy, critical thinking education, and improved moderation on social platforms. Addressing the underlying social and psychological factors that fuel belief in conspiracies is crucial for mitigating their impact on public discourse.

Keywords: Conspiracy Theories, Conspiracy Influencers, Social media, Echo chambers, Filter bubbles.

Introduction

Conspiracy theories are a social phenomenon that increasingly accompanies our lives and that finds fertile ground in the contemporary digital landscape. Although there are no studies that demonstrate that people believe conspiracy theories more or less than before, it is undeniable that the advent of social media and online sharing platforms has amplified the scope and speed with which such narratives spread, transforming marginal ideas into wide-ranging public discussions. In this context, "conspiracy influencers" play a fundamental role, acting as catalysts and amplifiers of theories that, despite lacking scientific basis, manage to fascinate millions of users.

This study hypothesizes that the success of conspiracy influencers in spreading misinformation is rooted in both cognitive biases and algorithmic amplification on social media platforms. This article seeks to answer the following research questions:

1) How do conspiracy influencers operate within digital ecosystems to promote and legitimize conspiracy theories?

2) What are the psychological and sociotechnical mechanisms that facilitate the work of these conspiracy influencers?

Through the strategic use of platforms such as YouTube, Instagram, TikTok and other social networks, these individuals manage to build a loyal following, exploiting persuasive communication mechanisms and captivating narratives. The phenomenon is particularly complex because it intertwines sociological, psychological and media aspects, raising relevant questions about how information circulates and consolidates in the collective mind.

Methodology

This study adopts a qualitative case study approach, combining thematic analysis with digital ethnography. The primary objective is to investigate how conspiracy influencers operate within online ecosystems, using the case of Cesare Sacchetti as a representative example. Rather than testing a hypothesis, this study seeks to identify patterns, rhetorical strategies, and cognitive mechanisms employed in the dissemination of conspiratorial content.

The main unit of analysis is Cesare Sacchetti's Telegram channel, chosen due to his prominence in the Italian conspiracy ecosystem and repeated mentions in international misinformation monitoring reports. His Telegram channel, which counts over 64,000 subscribers, serves as the main unit of analysis due to its high engagement and unfiltered content publication. Content posted between January and March 2025 was analysed using interpretive techniques informed by the theoretical framework outlined in sections 1 and 2. Analytical categories included use of emotional language, appeals to authority, and evidence of cognitive bias exploitation. While the sample is not exhaustive, it aims to illustrate patterns rather than provide statistical generalizations.

The analysis draws on theoretical frameworks outlined in the literature review, particularly psychological theories of conspiracy thinking and media studies perspectives on echo chambers and filter bubbles. No automated tools or computational methods were employed; the analysis is interpretative and grounded in close reading.

This study is not intended to provide statistical generalizations but rather to illustrate mechanisms through which conspiracy influencers operate. Limitations include the restricted time frame, the focus on a single platform (Telegram), and the absence of user-side data (such as engagement motivations or demographic profiles). Future research could expand on this foundation with comparative studies or mixed methods approaches incorporating audience interviews or social network analysis.

This study is limited by its reliance on publicly available content and does not include interviews or survey data. The analysis is illustrative rather than comprehensive, aiming to identify key patterns and mechanisms rather than establish generalizable claims.

Although this paper focuses on a single case (Cesare Sacchetti), the case is considered paradigmatic of broader dynamics within the conspiracy influencer ecosystem, making it suitable for an in-depth, illustrative analysis.

1. What is the phenomenon of conspiracy theories?

Unlike the reductionist collective imagination, conspiracy theories are not only elaborated by paranoid bearded outcasts with tin foil on their heads as a hat; the idea that a certain event is not simply the result of chance or the effect of unrelated causes, but of precise rational calculations elaborated by some shady figure acting in the shadows, is a flea present in the ear of man since ancient times, and it is a mechanism that can present itself in any person. Climate and environmental crises, pandemics, social and economic inequalities, scarcity of resources and raw materials; there are many who have stopped believing in progress. And the conflict, in conspiracy narratives, has now reached a supranational level; for this reason, depoliticization and conspiracy go hand in hand today.[1] Most attempts at refutation are ineffective, as everything is read as evidence of a global conspiracy, and the Enemy, whoever He is, a vacuous and intangible entity, is also ubiquitous, reducing the issue to a generalized us versus them.[2] And resentment seems to be the new opium of the people, the new narrative that dominates populism, crossing every threshold of ideology and political orientation.

Those who challenge the official versions, the media, the institutions and the world's leading experts in each field, do so by directly attacking those who hold power and knowledge; it is a political problem, a clear symptom of a widespread malaise and a crisis of and in contemporary democracy, of trust denied and placed in other personalities. Even the main tool with which attempts have been made to address the conspiracy phenomenon in recent decades, namely debunking, has almost never had the desired effects, when it has not even worsened the starting situation, making those who believe in these theories even more entrenched in their initial positions.

[1] D. Di Cesare, *Il complotto al potere*, Einaudi, Torino 2021, p. 77.
[2] Ibidem.

It is a common and widely shared opinion that the proliferation, if not the birth, of the conspiracy phenomenon was caused by the advent of the Internet[3]; the Internet has not only connected the entire world, it has not only informed, but also formed, and in addition to information, suspicion and conspiracy have also become global. However, this does not mean that conspiracy theories were born and grew with the advent of the Internet; it has simply benefited from it in terms of time and space in terms of the diffusion of the most recent theories, but if we look closely, we are talking about a phenomenon that has always existed and has played a role of primary importance throughout history.

From the studies of political scientists Joseph Uscinski and Joseph Parent, included in their book American Conspiracy Theories, where they analysed over one hundred thousand letters to the directors of the New York Times and the Chicago Times from 1890 to 2010 to understand how many times these theories were mentioned, it clearly emerges that the diffusion of such theories has been generally stable over time, with two significant peaks of short duration that occurred at the beginning of the twentieth century and at the beginning of the Cold War, in the years of greatest uncertainty in American public opinion and great changes, clearly observable in McCarthyism.[4] But it is enough to look back a couple of millennia to realize that conspiracy theories have always accompanied the public and private life of man.

For example, the entire history of Rome is pervaded by conspiracy narratives.[5] Often, they were used instrumentally by those in power for political purposes or to find a scapegoat, as in the case of Nero who, to defend himself from various accusations, placed the blame for the fire of Rome on the Christians in 64 AD.[6] A story that repeats itself, a red thread that unites and links different historical eras. On the Great Fire of London in 1666 that devastated the city for four days, the politician and writer Samuel Pepys wrote how from the very beginning there were pressing rumours of a plot behind the fire by Charles II, in a

[3] S. Stano, *The Internet and the Spread of Conspiracy Content*, in *Routledge Handbook of Conspiracy Theories*, Routledge, London 2020, p. 485.
[4] J. Uscinski and J. Parent, *American Conspiracy Theories*, Oxford University Press, New York 2014.
[5] V. Pagàn, *Conspiracy Narratives in Roman History*, University of Texas Press, Austin 2005.
[6] *The Great Fire of Rome: of fake news, conspiracy, and social disruption*, The Spirit of the Eye, 2021. https://visual-worlds.org/2021/07/23/the-great-fire-of-rome-of-fake-news-conspiracy-and-social-disruption/.

parallel between the sovereign and Nero, while others believed that the fire was started by internal enemies of England, such as the Catholics.

But what exactly is a conspiracy theory? There is no one-size-fits-all definition for all theories. According to the Oxford Learners Dictionaries, a conspiracy theory is when an event is hypothesized to have occurred as a result of a specific plan by a large organization.[7] However, following this path, one would not notice any substantial differences between a bank robbery and a September 11 conspiracy. Among the various definitions formulated by scholars who have dealt with the phenomenon, we cite two; according to Rob Brotherton, a conspiracy theory can be easily seen as the proposal of an idea that has not yet been, or cannot be, demonstrated. Furthermore, it consists of five main characteristics:

1) is a question that has not yet been answered;
2) starts from the general assumption that nothing is as it seems;
3) paints the conspirators as people with almost superhuman abilities;
4) the spasmodic and almost maniacal search for anomalies;
5) and finally, it is irrefutable.[8]

While Wu Ming 1, pseudonym of Roberto Bui, notes that not only have conspiracies always existed, exist and will exist in the future, but also that conspiracy theories of a political nature, different from those of a criminal nature, have the following characteristics:

1) they are created for a very specific purpose;
2) involve a limited number of actors;
3) they are put into practice imperfectly, because reality is imperfect;
4) they end once discovered and reported, which usually happens after a rather short period of time;
5) are inserted in their historical context and inseparably linked to it.[9]

[7] *Conspiracy theory*, Oxford Learners Dictionaries. https://www.oxfordlearnersdictionaries.com/definition/english/conspiracy-theory.
[8] R. Brotherton, *Menti sospettose: perché siamo tutti complottisti*, Bollati Boringhieri, Torino 2021, p. 75.
[9] Wu Ming 1, *Come nasce una teoria del complotto e come affrontarla, seconda parte*, Internazionale, 2018. https://www.internazionale.it/reportage/wu-ming-1/2018/10/29/teoria-complotto.

This last description corresponds to the political conspiracy par excellence, Watergate, which has given a suffix to many subsequent conspiracies: Irangate, Gamergate, Pizzagate, Pedogate.

Recent research has deepened our understanding of how conspiracy narratives adapt to and thrive within digital ecosystems. Phillips and Milner argue that online environments, particularly those that are participatory and memetic, are uniquely suited to the circulation of antagonistic and transgressive ideas, including conspiracy theories.[10] These platforms blur the lines between irony and belief, creating a discursive space where fringe ideas can gain traction and be rapidly amplified.

Marwick and Lewis, in their influential report on media manipulation, show how disinformation agents exploit the attention economy and platform algorithms to inject conspiracy narratives into mainstream discourse.[11] This manipulation is often framed through emotionally resonant content, making conspiratorial messaging especially "sticky" in online contexts.

Building on this, Rosenblum and Muirhead describe a shift toward a "new conspiracism" that abandons traditional evidence-based storytelling in favour of repetition, assertion, and social validation, dynamics that are exacerbated by social media.[12] These insights provide a crucial theoretical framework for understanding the mechanisms explored in the present analysis of conspiracy influencers.

2. Psychological aspects

As we have said, when dealing with the conspiracy phenomenon we must avoid falling into the error of believing that such theories are of interest only to a small paranoid fringe of humanity, made up of middle-aged, depressed or marginalized men, or that it is a question of wallet, class or cultural belonging.

[10] W. Phillips and R. M. Milner, *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*, Polity Press, Cambridge 2017.

[11] A. Marwick and Lewis R., *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017. https://datasociety.net/library/media-manipulation-and-disinfo-online/.

[12] R. Muirhead, N. L. Rosenblum and M. Landauer, *A Lot of People Are Saying: The New Conspiracism and the Assault on Democracy*, "Princeton University Press", 19(2): 142-174, 2019. http://dx.doi.org/10.1057/s41296-019-00372-6.

From the point of view of psychological studies, many authors have attributed the primary cause of the conspiracy phenomenon to “apophenia”. The term was coined by the German neurologist and psychiatrist Klaus Conrad in 1958 to describe the spontaneous, unmotivated observation of connections that is accompanied by a feeling of abnormal significance.[13] Basically, it describes the natural and innate tendency of our mind to connect situations and events that are apparently unrelated to each other, and to attribute meanings where there are none, without this necessarily indicating a pathological situation. Furthermore, it explains the attitude of those who are strongly convinced of a certain idea or theory and find confirmations of it around every corner, from numerology to tarot cards, to religions to various conspiracy theories. It allows you to find all the confirmations you need in the world.

But there are many other cognitive traps we can fall into, such as what in psychology is called confirmation bias[14], which can manifest itself when we are looking for evidence to verify our intuition and does not allow us to fairly weigh all the information we come across. The news we read most carefully, the links we click on, and the questions we ask ourselves, tend to align with what we already have in mind. Another rather insidious trap is the bias of proportionality[15]; when the outcome of an event is of significant and epochal significance, we need to believe that its cause was also something equally profound. Or, again, the bias of intentionality[16], a trigger-happy mechanism presents in each of us, which assumes that everything that happens in the world happens because someone wanted it. The tendency to judge a fact as intentional is automatic and does not require the slightest effort; the difficult thing, if anything, for our mind consists in making the effort to overcome this prejudice. As we can observe, there are many and varied traps into which one can fall.

[13] K. Rogers, *Apophenia*, Britannica, 2025. https://www.britannica.com/topic/apophenia.
[14] B. J. Casad, *Confirmation bias*, Britannica, 2025. https://www.britannica.com/science/confirmation-bias.
[15] I. Strauss Cohen, *The Psychology of Conspiracy Theories*, Psychology Today, 2025. https://www.psychologytoday.com/us/blog/your-emotional-meter/202401/the-psychology-of-conspiracy-theories.
[16] E. Rosset, *It’s No Accident: Our Bias for Intentional Explanations*, “Cognition”, 108(3):771-80, 2008. https://doi.org/10.1016/j.cognition.2008.07.001.

3. Internet as a Conspiracy Theory Amplifier

The advent of the Internet has radically transformed the way information is created, shared, and consumed. While this digital revolution has democratized access to knowledge, it has also facilitated the spread of conspiracy theories. Online platforms such as Facebook, Twitter, YouTube, and Reddit have become fertile ground for the proliferation of such narratives.[17]

The "echo chambers" are social or virtual environments where people surround themselves with individuals or content that confirms their beliefs, while actively avoiding conflicting sources of information. In other words, within these communities, ideas and opinions are continuously echoed without any criticism or alternative viewpoint. A practical example would be a Facebook group dedicated to a specific conspiracy theory, such as climate change denial. Users who participate in this group only share content that supports this view, reinforcing the belief that climate change is a hoax.[18] In essence, this is the virtual representation of the confirmation bias we talked about in the previous chapter.

In addition to these, there are also "filter bubbles", created by the algorithms of online platforms that personalize content based on the user's interactions and preferences. This mechanism limits exposure to different opinions and creates a homogeneous information environment. For example, a user who frequently watches conspiracy videos on YouTube will receive more and more suggestions for similar content, remaining trapped in a bubble in which all the information confirms his or her worldview.[19]

Different social media platforms have unique characteristics that influence the spread of conspiracy theories. For example, content moderation varies significantly between platforms: some adopt more restrictive policies, while others are more permissive.[20]

---

[17] M. Cinelli et al., *Conspiracy theories and social media platforms*, "Current Opinion in Psychology", 47:101407, 2022. https://doi.org/10.1016/j.copsyc.2022.101407.
[18] M. Cinelli et al., *The echo chamber effect on social media*, "Proceedings of the National Academy of Sciences of the United States of America", 2;118(9):e2023301118, 2021. https://doi.org/10.1073/pnas.2023301118.
[19] D. Spohr, *Fake news and ideological polarization: Filter bubbles and selective exposure on social media*, "Business Information Review", 34(3):150-160, 2017. https://doi.org/10.1177/0266382117722446.
[20] C. Körömi, P. Haeck and D. Cheslow, *Zuck goes full Musk, dumps Facebook fact-checking program*, Politico, 2025. https://www.politico.eu/article/mark-zuckerberg-full-elon-musk-dump-facebook-fact-checker/.

Removing content or users from one platform can lead to migration to other platforms with less moderation, a phenomenon known as “echo platforms,” deepening user segregation and further reinforcing conspiracy beliefs.

Repeated exposure to conspiracy theories can have significant psychological effects, including reduced trust in public institutions and increased perceptions of external threats.[21] Users who spend a lot of time in conspiracy-theory online communities tend to develop a collective identity based on shared narratives, thus strengthening a sense of belonging that makes it difficult to abandon these beliefs. Online polarization contributes significantly to the spread of conspiracy theories. When users interact primarily with homogeneous groups that share the same beliefs, an environment is created in which false information can spread rapidly without being challenged.[22] This reinforces existing beliefs and makes it more difficult to introduce correct information. Furthermore, the viral nature of social media allows conspiracy theories to reach a large audience quickly, increasing the potential for social harm.

4. The Conspiracy Influencers

Having explored how digital platforms facilitate the spread of conspiracy theories through cognitive and algorithmic mechanisms, we now turn to the role of individual actors, conspiracy influencers, who capitalize on these dynamics. The case of Cesare Sacchetti provides a concrete example of how these processes unfold in practice.

The Internet is full of personalities, pages and websites that spread conspiracy theories. In fact, some real conspiracy influencers are emerging with a large following. In Italy, a great example of these personalities is, as we mentioned above, Cesare Sacchetti, also known as “The most famous spreader of fake news”[23], whose Telegram channel alone has 64 thousand subscribers.[24]

[21] J. W. van Prooijen, G. Spadaro and H. Wang, *Suspicion of institutions: How distrust and conspiracy theories deteriorate social relationships*, 40(1): 65-69, 2022. https://doi.org/10.1016/j.copsyc.2021.06.013.
[22] Ibidem.
[23] *Il più celebre diffusore di fake news italiano ha colpito ancora*, Rolling Stones IT, 2022. https://www.rollingstone.it/politica/il-piu-celebre-diffusore-di-fake-news-italiano-ha-colpito-ancora/613475/.
[24] Link for the Telegram channel of Cesare Sacchetti: t.me/cesaresacchetti.

Its influence was certified last May by NewsGuard, an American company leader in monitoring disinformation on the web, which included it in the list of "super-spreaders of disinformation on Covid-19 in Europe".[25] Sacchetti is one of five Italians competing for the decidedly uncovered European primacy, together with the former Sicilian coordinator of the Lega Patrizia Rametta, the former head of communications for the 5 Star Movement in the Senate Claudio Messora (known on the internet for his blog Byoblu), the current M5S senator Elio Lannutti and Alessandro Meluzzi, a former member of parliament for Forza Italia, now a regular on television talk shows.

A graduate in European Studies and with a never completed doctorate in public law, he began his career collaborating with blogs and newspapers such as "Il Fatto Quotidiano" and "Il Giornale", often dealing with Eurosceptic issues and supporting Donald Trump. Since 2020, with the global health emergency, Sacchetti has gained notoriety by denouncing alleged conspiracies linked to the pandemic, such as the involvement of Bill Gates and the "New World Order". He has become a leading Italian proponent of the QAnon theory, producing content about a supposed international paedophile elite, and linking Italian and international political figures to conspiracies against Trump. His online activity has seen significant growth, with a 52% increase in Twitter followers during the pandemic.

But why are we talking about him so much? Because by looking at his telegram channel you can see exactly how a conspiracy influencer spreads his content, taking advantage of the vulnerability of his audience. Most of the time, people do not have the skills or time to verify every piece of information they meet, due to the Infodemic. Well, these influencers can exploit this vulnerability to gain a large following, combined with a psychological predisposition of some individuals to look askance at mainstream media and common narratives.

Let's take as an example this "news" spread on his Telegram channel on March 24, 2025:

[25] S. Fontana, *Chi è Cesare Sacchetti, il re dei complottisti italiani*, Rolling Stones, 2021. https://www.rollingstone.it/politica/chi-e-cesare-sacchetti-il-re-dei-complottisti-italiani/548167/.

Figure 1. *Screenshot of Telegram content on Cesare Sacchetti's channel. Unfortunately, it is only possible to provide the link to the Telegram channel: t.me/cesaresacchetti.*

In the message, Obama and Clooney are accused of paedophilia against the little girl who is with them on the boat, reprising a theme dear to the QAnon orbit that sees leading figures of the left as the biggest paedophiles in the world. Now, it is enough to do a check on Google Images, to see how the photo, which does not prove anything, is just one of many taken on that boat trip on Lake Como in 2019, in which many other people are present. Among other things, the meeting in question between Clooney and Obama in northern Italy, near the actor's property in the area, has been widely covered by various media outlets.[26]

[26] A. Zilber, *The Obamas join the Clooneys aboard a boat on Lake Como as the former first family attend a glamorous event hosted by the Hollywood star's charity near his multi-million dollar Italian mansion*, Daily Mail, 2019. https://www.dailymail.co.uk/news/article-7172965/Barack-Obama-George-Clooney-look-dressed-business-sail-boat-Italy.html.

Figure 2. *Source: https://maldita.es/malditobulo/20220520/clooney-obama-pedofilos-secuestrar-nina/.*

Figure 3. *Source: https://www.instagram.com/p/BzEn7RqlDq3/?utm_source=ig_embed.*

Sacchetti's messaging aligns closely with apophenic thinking, where unrelated events (e.g., a boat trip photo) are imbued with conspiratorial significance. Moreover, his appeal is amplified through the formation of parasocial relationships, wherein followers perceive a sense of personal connection and trust, reinforcing the authority of his claims despite lack of evidence.

Now, Sacchetti is a highly educated individual, regularly registered in the register of journalists and with several years of experience in the field. Given these premises, it is difficult to believe that he does not know that he is spreading a totally false and decontextualized news, something that some users also point out to him among the 415 comments.

This allows us to clearly distinguish between misinformation and disinformation: misinformation means the dissemination of false or incorrect information without the intention of deceiving, since one truly believes in what is said or written. It can arise from

errors, misunderstandings or lack of verification of sources. On the contrary, disinformation is the deliberate dissemination of false information with the aim of deceiving, manipulating or influencing public opinion.[27]

Before going further, however, it is good to specify that, while Sacchetti offers a particularly vivid example, similar patterns are observable in other conspiracy influencers across Europe, such as Xavier Azalbert[28] in France or Attila Hildmann[29] in Germany, who combine alternative health narratives with political conspiracy rhetoric.

5. Countering and Preventing Conspiracy Theories

Conspiracy theories represent a significant challenge in contemporary society, with implications ranging from public health to political stability. To effectively address this phenomenon, it is necessary to adopt counter- and prevention strategies based on scientific evidence and supported by authoritative academic sources.

Education plays a crucial role in preventing adherence to conspiracy theories. Promoting critical thinking in schools and universities helps individuals develop the analytical skills needed to evaluate the reliability of information. Providing teachers with adequate tools to address conspiracy theories in the classroom is essential to building a cultural resistance against misinformation. Furthermore, studies have shown that teaching analytical thinking skills can significantly reduce belief in conspiracy theories.[30]

Social media platforms are often primary vectors for the spread of conspiracy theories. It is crucial that these platforms implement measures to identify and limit the propagation of false or misleading content. Research indicates that social media use is correlated with the spread of conspiracy beliefs, especially among those who already show a propensity

---

[27] J. Palfrey, *Misinformation and disinformation*, Britannica, 2025. https://www.britannica.com/topic/misinformation-and-disinformation.

[28] P. R. Korda, *Xavier Azalbert, le pro de la finance qui a fait de France Soir un site complotiste*, Le Parisien, 2024. https://www.leparisien.fr/culture-loisirs/tv/france-soir-comment-ce-grand-titre-populaire-est-devenu-un-site-complotiste-25-01-2021-8421114.php.

[29] L. Morris and W. Glucroft, *Prospect of a coronavirus vaccine unites anti-vaxxers, conspiracy theorists and hippie moms in Germany*, The Washington Post, 2020. https://www.washingtonpost.com/world/europe/coronavirus-vaccine-anti-vaxx-germany/2020/07/02/da7efc7e-acba-11ea-a43b-be9f6494a87d_story.html.

[30] C. O'Mahony et al., *The efficacy of interventions in reducing belief in conspiracy theories: A systematic review*, "Public Library of Science One", 5;18(4), 2023. https://doi.org/10.1371/journal.pone.0280902.

towards such ideas. Therefore, improving algorithmic transparency and promoting fact-checking can help mitigate the impact of online conspiracy theories.[31]

Actively engaging local communities is another key element in the fight against conspiracy theories. Initiatives that promote collaborative debunking and open discussion can help dismantle false beliefs. For example, educational programs that use real testimonies to show the negative effects of extremism have proven to be effective in raising awareness among young people. Creating safe spaces for dialogue and providing tools to recognize and challenge disinformation are key steps in this process.[32]

Academic research provides in-depth understanding of the psychological and social motivations that lead individuals to embrace conspiracy theories. Studies have shown that a sense of lack of control can increase the likelihood of believing in such theories, while interventions that strengthen a sense of personal control can reduce this tendency. Furthermore, research highlights the importance of addressing conspiracy theories through an educational approach, rather than simple refutation, to avoid the effects of reinforcing incorrect beliefs.[33]

Conclusions

Considering the analyses conducted, it is clear that conspiracy influencers play a key role in the proliferation of online conspiracy theories. Their ability to construct a coherent narrative, often based on emotional and sensational elements, allows them to capture the attention of a large and diverse audience. The combination of personal charisma, convincing rhetoric and exploitation of the audience's cognitive weaknesses makes these individuals particularly effective in spreading ideas that are not supported by empirical evidence.

[31] A. M. Enders et al., *The Relationship Between Social Media Use and Beliefs in Conspiracy Theories and Misinformation*, "Political Behavior", 45(2):781-804, 2023. https://doi.org/10.1007/s11109-021-09734-6.
[32] A. Phoenix, *Combatting Extremism and Conspiracy Theories in the Classroom*, Educate Against Hate, 2022. https://www.educateagainsthate.com/blog/posts/combatting-extremism-and-conspiracy-theories-in-the-classroom/.
[33] L. Jerome, B. Kisby and S. McKay, *Combatting conspiracies in the classroom: Teacher strategies and perceived outcomes*, "British Educational Research Journal", Volume 50, Issue 3, Pages 1106-1126, 2024. https://doi.org/10.1002/berj.3955.

However, their impact goes beyond simple misinformation: they contribute to creating cohesive and polarized virtual communities, in which the conspiracy vision becomes an integral part of individual and collective identity. Countering this phenomenon requires not only a greater commitment from digital platforms in monitoring content, but also widespread education aimed at promoting critical thinking and digital awareness. Only through a deep understanding of the social and psychological dynamics involved will it be possible to stem the influence of conspiracy influencers and promote a more balanced and transparent information ecosystem.

This study is limited by its focus on a single case study and a narrow time frame. While the analysis offers valuable insight into the mechanisms and strategies employed by conspiracy influencers, it does not provide a generalizable model. Furthermore, the study relies exclusively on publicly available content, without incorporating audience perspectives or engagement metrics. Future research could expand this analysis through comparative case studies across different cultural contexts or by employing mixed methods, including user interviews, discourse analysis, and network mapping. Such approaches would provide a more comprehensive understanding of how conspiracy narratives circulate and consolidate within digital environments.

References

A. M. Enders et al., *The Relationship Between Social Media Use and Beliefs in Conspiracy Theories and Misinformation*, "Political Behavior", 45(2):781-804, 2023. https://doi.org/10.1007/s11109-021-09734-6.

C. O'Mahony et al., *The efficacy of interventions in reducing belief in conspiracy theories: A systematic review*, "Public Library of Science One", 5;18(4), 2023. https://doi.org/10.1371/journal.pone.0280902.

D. Di Cesare, *Il complotto al potere*, Einaudi, Torino 2021.

D. Spohr, *Fake news and ideological polarization: Filter bubbles and selective exposure on social media*, "Business Information Review", 34(3):150-160, 2017. https://doi.org/10.1177/0266382117722446.

E. Rosset, *It's No Accident: Our Bias for Intentional Explanations*, "Cognition", 108(3):771-80, 2008. https://doi.org/10.1016/j.cognition.2008.07.001.

J. Uscinski and J. Parent, *American Conspiracy Theories*, Oxford University Press, New York 2014.

J. W. van Prooijen, G. Spadaro and H. Wang, *Suspicion of institutions: How distrust and conspiracy theories deteriorate social relationships*, 40(1): 65-69, 2022. https://doi.org/10.1016/j.copsyc.2021.06.013.

L. Jerome, B. Kisby and S. McKay, *Combatting conspiracies in the classroom: Teacher strategies and perceived outcomes*, "British Educational Research Journal", Volume 50, Issue 3, Pages 1106-1126, 2024. https://doi.org/10.1002/berj.3955.

M. Cinelli et al., *Conspiracy theories and social media platforms*, "Current Opinion in Psychology", 47:101407, 2022. https://doi.org/10.1016/j.copsyc.2022.101407.

M. Cinelli et al., *The echo chamber effect on social media*, "Proceedings of the National Academy of Sciences of the United States of America", 2;118(9):e2023301118, 2021. https://doi.org/10.1073/pnas.2023301118.

R. Brotherton, *Menti sospettose: perché siamo tutti complottisti*, Bollati Boringhieri, Torino 2021.

R. Muirhead, N. L. Rosenblum and M. Landauer, *A Lot of People Are Saying: The New Conspiracism and the Assault on Democracy*, "Princeton University Press", 19(2): 142-174, 2019. http://dx.doi.org/10.1057/s41296-019-00372-6.

S. Stano, *The Internet and the Spread of Conspiracy Content*, in *Routledge Handbook of Conspiracy Theories*, Routledge, London 2020, p. 485.

V. Pagàn, *Conspiracy Narratives in Roman History*, University of Texas Press, Austin 2005.

W. Phillips and R. M. Milner, *The Ambivalent Internet: Mischief, Oddity, and Antagonism Online*, Polity Press, Cambridge 2017.

Sitography

A. Marwick and Lewis R., *Media Manipulation and Disinformation Online*, Data & Society Research Institute, 2017. https://datasociety.net/library/media-manipulation-and-disinfo-online/.

A. Phoenix, *Combatting Extremism and Conspiracy Theories in the Classroom*, Educate Against Hate, 2022. https://www.educateagainsthate.com/blog/posts/combatting-extremism-and-conspiracy-theories-in-the-classroom/.

A. Zilber, *The Obamas join the Clooneys aboard a boat on Lake Como as the former first family attend a glamorous event hosted by the Hollywood star's charity near his multi-million dollar Italian mansion*, Daily Mail, 2019. https://www.dailymail.co.uk/news/article-7172965/Barack-Obama-George-Clooney-look-dressed-business-sail-boat-Italy.html.

B. J. Casad, *Confirmation bias*, Britannica, 2025. https://www.britannica.com/science/confirmation-bias.

C. Körömi, P. Haeck and D. Cheslow, *Zuck goes full Musk, dumps Facebook fact-checking program*, Politico, 2025. https://www.politico.eu/article/mark-zuckerberg-full-elon-musk-dump-facebook-fact-checker/.

Conspiracy theory, Oxford Learners Dictionaries. https://www.oxfordlearnersdictionaries.com/definition/english/conspiracy-theory.

I. Strauss Cohen, *The Psychology of Conspiracy Theories*, Psychology Today, 2025. https://www.psychologytoday.com/us/blog/your-emotional-meter/202401/the-psychology-of-conspiracy-theories.

Il più celebre diffusore di fake news italiano ha colpito ancora, Rolling Stones IT, 2022. https://www.rollingstone.it/politica/il-piu-celebre-diffusore-di-fake-news-italiano-ha-colpito-ancora/613475/.

J. Palfrey, *Misinformation and disinformation*, Britannica, 2025. https://www.britannica.com/topic/misinformation-and-disinformation.

K. Rogers, *Apophenia*, Britannica, 2025. https://www.britannica.com/topic/apophenia.

L. Morris and W. Glucroft, *Prospect of a coronavirus vaccine unites anti-vaxxers, conspiracy theorists and hippie moms in Germany*, The Washington Post, 2020. https://www.washingtonpost.com/world/europe/coronavirus-vaccine-anti-vaxx-germany/2020/07/02/da7efc7e-acba-11ea-a43b-be9f6494a87d_story.html.

P. R. Korda, *Xavier Azalbert, le pro de la finance qui a fait de France Soir un site complotiste*, Le Parisien, 2024. https://www.leparisien.fr/culture-loisirs/tv/france-soir-comment-ce-grand-titre-populaire-est-devenu-un-site-complotiste-25-01-2021-8421114.php.

S. Fontana, *Chi è Cesare Sacchetti, il re dei complottisti italiani*, Rolling Stones, 2021. https://www.rollingstone.it/politica/chi-e-cesare-sacchetti-il-re-dei-complottisti-italiani/548167/.

The Great Fire of Rome: of fake news, conspiracy, and social disruption, The Spirit of the Eye, 2021. https://visual-worlds.org/2021/07/23/the-great-fire-of-rome-of-fake-news-conspiracy-and-social-disruption/.

Wu Ming 1, *Come nasce una teoria del complotto e come affrontarla, seconda parte*, Internazionale, 2018. https://www.internazionale.it/reportage/wu-ming-1/2018/10/29/teoria-complotto.

„dot.pl" - czasopismo Rejestru domeny .pl

Sport w epoce cyfrowej. Zróżnicowane wymiary rywalizacji

Konrad Burdyka
Instytut Nauk Socjologicznych i Pedagogiki, Szkoła Główna Gospodarstwa Wiejskiego, Polska
ORCID: https://orcid.org/0000-0002-5723-2019
E-mail: kburdyka@wp.pl

Received: 19.12.2025
Accepted: 19.12.2025
Published: 19.12.2025

Cite this article as:
K. Burdyka, "*Sport w epoce cyfrowej. Zróżnicowane wymiary rywalizacji*"

DOT.PL, no. 1/ 2025,
10.60097/DOTPL/215871

Corresponding author:
Kobrad Burdyka, Instytut Nauk Socjologicznych i Pedagogiki, Szkoła Główna Gospodarstwa Wiejskiego, Polska

E-mail: kburdyka@wp.pl

Streszczenie

Tekst stanowi sprawozdanie z konferencji „„Społeczny wymiar sportu w Polsce. Między wspólnotą, kulturą a polityką", zorganizowanej w Warszawie w listopadzie 2025 r. W ramach wydarzenia debatowano nt. wpływu sportu na życie społeczne. Podkreślono znaczenie e-sportu i szachów dla rozwoju kompetencji cyfrowych i ich potencjalny wpływ na szeroko rozumianą sferę bezpieczeństwa. Wydarzenie zrealizowano w ramach projektu "Obserwatorium Społecznego Oddziaływania Sportu", prowadzonego przez Fundację Wespół i finansowanego przez NIW-CRSO.

Słowa kluczowe: e-sport, Obserwatorium Społecznego Oddziaływania Sportu, konferencja naukowa

Sport in the digital age. Varied dimensions of rivalry

Abstract

The text presents a report on the conference “The Social Dimension of Sport in Poland: Between Community, Culture and Politics” held in Warsaw in November 2025. The event focused on discussions concerning the impact of sport on social life. Particular emphasis was placed on the role of e-sports and chess in the development of digital competencies and their potential influence on the broadly understood sphere of security. The conference was organised as part of the Observatory for the Social Impact of Sport (run by the Wespół Foundation), financed by the National Freedom Institute – Center for Civil Society Development.

Keywords: e-sports, the Observatory for the Social Impact of Sport, academic conference

21 listopada br. odbyła się w Szkole Głównej Gospodarstwa Wiejskiego w Warszawie konferencja naukowa „Społeczny wymiar sportu w Polsce. Między wspólnotą, kulturą a polityką”. Wydarzenie zorganizowała Fundacja Wespół oraz Instytut Nauk Socjologicznych i Pedagogiki SGGW. Konferencja zgromadziła badaczy i praktyków zainteresowanych sportem jako zjawiskiem wykraczającym daleko poza sferę aktywności fizycznej – obejmującym również wymiar kulturowy, technologiczny i edukacyjny. Dzięki interdyscyplinarnemu charakterowi debata stanowiła ważny głos w dyskusji o przyszłości sportu w dobie cyfrowej transformacji.

Konferencja zwieńczyła prace badawcze realizowane w ramach projektu Obserwatorium Społecznego Oddziaływania Sportu (OSOS), prowadzonego przez Fundację Wespół dzięki środkom Rządowego Programu Rozwoju Organizacji Obywatelskich na lata 2018-2030. Głównym celem przedsięwzięcia było wypełnienie luki badawczej w obszarze empirycznych analiz wpływu sportu na życie społeczne i lokalne

wspólnoty w Polsce. Dużo uwagi poświęcono problemom, z którymi mierzą się kluby sportowe w Polsce.

Jednym z istotnych wątków, który podjęto w czasie konferencji była refleksja nad **e-sportem** jako formą rywalizacji opartej na kompetencjach poznawczych, refleksie, analizie danych i strategicznym myśleniu. Dyskusje te jednoznacznie pokazywały, że zjawiska sportu nie można ograniczyć dziś wyłącznie do wysiłku fizycznego, lecz wymaga on również intensywnej pracy umysłowej, często realizowanej w środowisku cyfrowym.

W swoim wystąpieniu dr. Michał Jasny (AWF Józefa Piłsudskiego w Warszawie) zwrócił uwagę na dynamiczny rozwój rywalizacji gamingowej oraz jej ambiwalentny charakter. Z jednej strony e-sport generuje nowe ścieżki rozwoju kompetencji cyfrowych, pracy zespołowej i analitycznego myślenia, z drugiej – rodzi pytania o uzależnienia, presję performatywności, komercjalizację oraz bezpieczeństwo młodych użytkowników w sieci.

Cennym uzupełnieniem ww. perspektywy był referat dr. Jakuba Stempnia (Uniwersytet Łódzki) dotyczący sytuacji szachistek-amatorek w Polsce. Referat unaocznił, że sporty umysłowe – choć często postrzegane jako neutralne i egalitarne – również podlegają mechanizmom nierówności płciowych. Jednocześnie szachy, podobnie jak e-sport, stanowią istotne pole rozwoju kompetencji poznawczych, strategicznych i edukacyjnych wśród młodego pokolenia, coraz częściej przenoszonych do środowisk cyfrowych i platform online.

W kontekście bezpieczeństwa interesujące było również wystąpienie dr. Dobrosława Mańkowskiego (Uniwersytet Gdański) poświęcone potencjałowi proobronnemu klubów sportowych. Choć dotyczyło ono głównie tradycyjnych form rywalizacji sportowej, jego wnioski można odnieść również do środowisk graczy komputerowych, które coraz częściej funkcjonują jako sieciowe wspólnoty zdolne do szybkiej mobilizacji, transferu wiedzy i kompetencji – także tych przydatnych w obszarze szeroko rozumianego bezpieczeństwa państwa.

Warto podkreślić, że konferencja wpisywała się w szerszy nurt działań Fundacji Wespół, która – obok działalności integracyjnej i edukacyjnej – przygotowuje serie raportów problemowych. W jednym z najnowszych opracowań nt. **„E-sport jako zjawisko społeczne. Szanse i zagrożenia”** w przystępnej, popularnonaukowej formie podjęte zostaną kluczowe kwestie związane z rozwojem rywalizacji gamingowej i jej wpływu na

młode pokolenie, jak również potencjalnym znaczeniem e-sportu dla kształtowania kompetencji cyfrowych, analitycznych i związanych z szeroko rozumianą sferą obronności.