Anna Makuch[*]
Nicola Strizzolo[**]

The Social Dimension of Cybersecurity in the Public Media Systems of Poland and Italy

Abstract

This paper explores the social dimension of security concerning public broadcasters in Poland and in Italy. Public broadcasters are obliged to design their content around a mission. This is a requirement under national regulations on state security. From the perspective of national systems with legal and political histories as different as Poland's and Italy's, the shaping of the social space by public broadcasters' digital tools reflects the transnational vector of action based on public media.

Key words: media system, cybersecurity, social security, international relations, international cooperation

[*] Anna Makuch, PhD, Faculty of Social Sciences, University of Economics and Human Sciences in Warsaw, e-mail: a.makuch@vizja.pl, ORCID: 0000-0002-5222-4407.

[**] Prof. Nicola Strizzolo, University of Udine, Department of Human Sciences, e-mail: nstrizzolo@unite.it, ORCID: 0000-0001-6384-9210.

Preliminary assumptions – conceptualisation

Since the beginning of the nineteenth century, the human security environment has undergone changes, leading to a significant expansion of the subject catalogue of areas requiring systemic action by state actors. The military factor that for centuries was a guarantee of border protection and a tool of (defensive and offensive) foreign policy (e.g., the Roman Empire) in the structure of state activity gradually began to lose its leading position, directing the attention of states to economic, technological or cultural factors (soft and smart power[1]). The concept of power in international relations still determines the level of causality of actors in the realisation of values and interests, while the utility of the tools and means that create power is the result of the assets individually developed by the actors, corresponding to the potential of states. There is a group of factors that constitute an obligatory tool for the conduct of domestic or foreign policy – and in view of the considerable networking of human relations, the burden of attention of any actors in international relations is focused on communication resources, which are decisive in determining the hierarchy of power[2]. The control of the information environment in the pursuit of interests is not the domain of the current digital age – during the period of the propaganda narratives of totalitarian states, it became evident that the future of power would be linked to influencing public opinion[3]. Nowadays, given the importance of cyberspace, establishing rules for functioning in virtual reality, in view of the fundamental goals of the state, is a challenge that necessarily attracts the attention of states and the international community.

Social security from a cybernetic perspective[4] refers to maintaining the ability to activate defence mechanisms in the event of threats. Maintaining an equilibrium requires maintaining the functionality of regulators that influence the so-called ultra-stability of the system[5]. In the case of society, the regulators are people although, within society, there are smaller structures within which the principle of homeostasis also operates (companies, enterprises, etc.). The regulator of the social security system in the state is the legislative-executive-

[1] J.S. Nye Jr, *Soft Power: The Means to Success in World Politics*, New York 2002.

[2] M. Castells, *Władza komunikacji*, Warszawa 2013, p. 25.

[3] E.L. Bernays, *Propaganda*, New York 1928, p. 9.

[4] M. Mazur, *Homeostaza społeczna* [in:] *Procesy samoregulacji w oświacie. Problemy homeostazy społecznej*, eds.. M. Pęcherski, J. Tudrej, Warszawa 1983, p. 107.

[5] W. Ross Ashby, *Design for a brain. The origin of adaptative behaviour*, New York 1960, p. 98.

judicial power with a monopoly of violence in the event of violations of the rules and principles of public order. Strategic goals, policy and regulatory measures in the Polish national legal system are defined in the Cybersecurity Strategy for 2019–2024[6].

The Cybersecurity Strategy addresses the public, military, and private levels, framed by five specific objectives, i.e., developing the national security system, enhancing resilience and response, increasing national technological capabilities, building public awareness and competence, and strengthening Poland's position on the international arena as a strong cyberplayer.

The social dimension is captured by Goal 4, point 8.3 of the Cybersecurity Strategy, i.e., „Developing public awareness towards the safe use of cyberspace", which includes a recommendation for public-private cooperation in the field of education for the safe use of cyberspace in the technological (data security) and information fields.

In the Polish scientific tradition, social security is the domain of international security, and further – national security [„Social security is associated with the probability of undesirable phenomena (problems) and the reduction of risks related to the survival and quality of life in the economic and cultural spheres"[7]]. Normative acts define social security as securing citizens' life, health and property (Art. 67 of the Polish Constitution[8]). In contrast, securology perceives social security far more broadly – in juxtaposition with the most pressing challenges related to threats to the functioning of the state. It seems that the essence of social security is to guarantee conditions for the free and risk-free development of members of society, assuming the elimination of external and internal threats, and this is the idea expressed by the National Security Strategy of the Republic of Poland. According to the Strategy, social security includes the following components: social security, the protection of national heritage, education for security, media for security, and demographic changes.

The purpose of this publication is to determine how the goal of maintaining social security in the context of cyberspace is defined by the public media of designated state entities in their strategies and policy documents. Public

[6] Cybersecurity Strategy of the Republic of Poland 2019–2024 (Official Gazette of the Republic of Poland 2019, item. 1037). See also M. Karpiuk, A. Makuch, U. Soler, *The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity*, „Polish Political Science Yearbook" 2023, no. 3.

[7] J. Gierszewski, *Bezpieczeństwo społeczne jako dziedzina bezpieczeństwa narodowego*, „Historia i Polityka" 2018, no. 23, p. 22.

[8] Constitution of the Republic of Poland (Journal of Laws 1997, no. 78, item 483).

media in the legal and political systems are a vehicle and tool of policies – both domestic and foreign – of the state, the primary goal of which is the security and development of citizens. Hence, their role in shaping the social security environment is significant, if not crucial. It is assumed[9] that the processes of social homeostasis are influenced by organisations with the ability to give orders and enforce them (public media – strategy – implementation of this strategy through the production, selection and distribution of messages – programs, broadcasts, advertisements).

The article uses the critical-analytical method with elements of the dogmatic-legal method. This made it possible to analyse and evaluate the solutions adopted at the level of the public media system, remaining a subsystem of the legal and political system of state entities, i.e., Italy and Poland. Given the strong trend of the internationalisation of interstate relations (e.g., within the EU) and transnational threats in the security sphere, the comparativeness of the indicated issue is characterised by a strong potential for evaluation of current and future actions.

The mission of public media in the field of social security Poland – principles, bases, program documents

The tasks of public media in Poland are regulated by Art. 21 of the Broadcasting Act[10], qualitatively and quantitatively indicating the main implementation directions. In the general part, i.e., Art. 1.3a, there is a provision for disseminating civic education through the radio and television channels of the Polish media system. The tasks of the public media are specified in Chapter 4, Art. 21 of the Act. More specifically, Par. 1 imposes the obligation to provide a diverse, unbiased and technologically high-quality information, cultural, educational, and entertainment offer. Pluralism finds concretisation not only in terms of the perspectives of content presentation or the number of channels, but it also applies to differentiation in terms of parts of society (8a). In Par. 1a.1, 1a.2 and 1a.9 of Art. 21, the legislator specifies the task of profiling the offer in terms of local or specialised audiences. Here, it also gives expression to the mission of public television as a tool of foreign policy through the presence of

[9] M. Mazur, op. cit.

[10] Broadcasting Act of 29 December 1992 (Journal of Laws 2022, item 1722).

an offer aimed at foreign audiences in languages other than Polish. Paragraphs 2a and 2b formulate tasks corresponding to digital technologies that have introduced contact between broadcasters and viewers, and personalised on-demand channels as the standard of modern media. Public media are charged with the duty of care for the construction and maintenance of broadcasting infrastructure (Par. 3) and technical innovation (Par. 5). Public media, under Par. 1a.6a, are obliged to archive and take care of resources, which also includes improving quality according to technological possibilities. Paragraphs 1a.8 and 1a.9 specify the tasks of protecting national heritage and national identity in accordance with the National Strategy of the Republic. In the framework of combating social exclusion, public media have an obligation (Art. 21 Par. 1a.10) to prepare content in a manner accessible to people with disabilities.

The principles of the public media in Poland, in accordance with Art. 21(2) of the Broadcasting Act, are as follows: accountability, reliability, orientation towards the free formation of public opinion, enabling the principle of participation in social and political life, protection and promotion of Polish culture, integration of Polish society, as well as promoting science, culture, knowledge and sports, universal Christian principles, family and media education.

Thus formulated, the goals and methods correspond to the principle of social security of the Polish nation and state while meeting the conditions corresponding to the cultivation of a democratic political culture based on access to pluralised information supporting attitudes of participation in the governance and control of power[11].

The study included Polskie Radio and TVP Info services in 2022. TVP Info is Telewizja Polska's news channel, which broadcasts regional programming from all regional branches in Poland. Polskie Radio is a sole-shareholder company of the State Treasury assigned with public tasks fulfilled through Polish – and foreign-language news websites. Polskie Radio's channels usually rank fourth, fifth or sixth out of twenty-two in terms of listening figures in Poland (except for the Pomeranian and West Pomeranian Voivodeships – eleventh and ninth

[11] Cf.: J. Garlicki, A. Noga-Bogomilski, *Kultura polityczna w społeczeństwie demokratycznym*, Warszawa 2004, p. 18–23; I. Kamińska-Szmaj, *Co to jest kultura polityczna?* [in:] *Język a kultura*, vol. 11, *Język polityki a współczesna kultura polityczna*, eds. J. Anusewicz, B. Siciński, Wrocław 1994; W. Lamentowicz, *Państwo współczesne*, Warszawa 1993, p. 61–64.

position, respectively[12]). This is a strong performance given the broadcaster's public remit – Polskie Radio does not offer mass entertainment, focusing instead on high-culture content.

Telewizja Polska S.A. provides 236 audiovisual services[13], including 21 nationwide channels, one in English. The issue of cybersecurity on a social scale is devoted to news services and educational programs – episodes („Full picture". Season 2. Cybersecurity – 18.10.2022, 27 minutes), information and social campaigns (the promotion of NASK's cybersecurity vademecum in advertising blocks of premium time[14]).

In 2022, the TVP 1 station led in audience figures, followed by Polsat, TVP 2 and TVN[15]. TVP INFO occupied the sixth position, with a 30,40% increase in viewership. Last year, TVP INFO had forty-six archived and available items about the social aspects of cybersecurity. Content from TVP INFO's website is published on Polskie Radio's website. The content aired on television has a larger component on state security and the international perspective.

Polskie Radio's content related to cybersecurity is archived and kept freely available in chronological order, from the latest to the oldest. The archive contains material spanning ten years. In 2022, cybersecurity was the subject of 181 publications and broadcasts. The cybersecurity category encompasses issues around information and personal data protection, international relations, the latest cybertechnologies, important information about state matters with regard to law, and political and administrative decisions. Polskie Radio's task is to inform the public and to publish educational (including popular science) content through neutrally formulated reports and messages that cover the subject comprehensively. The choice of subjects corresponds to the current issues around the state's domestic and foreign affairs. Archived broadcasts fulfil public security objectives by means such as raising awareness

[12] M. Kurdubski, *RMF FM liderem słuchalności we wszystkich województwach. Mapa radiowa Polski*, https://www.wirtualnemedia.pl/artykul/mapa-radiowa-polski-sluchalnosc-radia-w-wojewodztwach-dane-2022-rok [access: 5.09.2023].

[13] https://s.tvp.pl/repository/attachment/5/2/2/522e786f6dcff8fbf34fdc1e36df78221670338773202.pdf [access: 5.09.2023].

[14] Cf. *Kampanie edukacyjno-informacyjne na rzecz upowszechnienia korzyści z wykorzystywania technologii cyfrowych*, https://www.nask.pl/pl/projekty-dofinansowane/projekty-ue/3822,Kampanie-edukacyjno-informacyjne-na-rzecz-upowszechnienia-korzysci-z-wykorzystan.html [access: 5.09.2023].

[15] *TVP1 liderem rankingu oglądalności w 2022 r. Wyraźny wzrost TVP Info*, https://www.tvp.info/65442798/ranking-ogladalnosci-stacji-telewizyjnych-w-polsce-w-2022-roku-tvp1-liderem-polsat-drugi-tvp2-zamyka-podium-[access: 5.09.2023].

about cyberthreats (phishing, identity theft, investment fraud, e-prescribing fraud), announcing security alerts about compromised international security (attacks against critical state infrastructure, cyberattacks, e.g., against Ukrainian businesses) and promoting cybersecurity hygiene, as well as the basic rules of internet use. Target audiences span all age and occupational groups – for instance, materials about protecting intimate content for young users, content promoting internet safety for seniors, and warnings about apps for World Cup football fans in Qatar. Therefore, Polskie Radio fulfils its mission as a public broadcaster by addressing the issue of cybersecurity from many different angles, primarily with the Polish public mind. At the same time, the broadcaster promotes universal values based on democratic principles of legal egalitarianism, freedom of speech, participation in exercising and controlling power, and access to transparent information.

The mission of public media in the field of social security in Italy – principles, bases, program documents

For the Italian issue, we must first make a semantic difference. Namely, social security has a different meaning than the meaning rightly used by my colleague in her context. In Italy, „social security" is synonymous with „social protection" and concerns social assistance to protect the poor, and social security to protect workers[16].

In Italian, for the topic of the text, we have to refer to the term „public safety", which is commonly understood as the set of tasks attributed to the authorities in charge of maintaining public order, the safety and security of citizens, the protection of property, and the control and observance of laws and regulations, and the authorities that are also entrusted with public rescue operations in the event of public and private accidents. These tasks are handled by the various authorities and services in charge of public safety, which operate at national, provincial and local levels.

Bringing the concept to telecommunications, public safety should be addressed to radio, television and the internet, with distinctions between public and private, broadcasting over the air and the web. Although the history

[16] A. Garilli, *La sicurezza sociale degli immigrati: alla ricerca della solidarietà perduta*, Bologna 2020.

of the laws intertwines with that of the sensitivity and culture of the issues they regulate, for the sake of the economy of the text, we only refer to the present or more recent years.

Constitutional Court's ruling No. 102/1990 established that radio and television installations use a limited common good – the airwaves – and require an allocation of a frequency band, thus distinguishing themselves from the press. The reference law for frequency management is Law No. 223/1990, known in Italy as the Mammì Law, from its parliamentary promoter, the Honourable Oscar Mammì[17]. The law has seen a long gestation, in the events related to the birth and spread of private broadcasters, to great public debates, and continuous and intersecting court cases. At the heart of this arrangement is pluralism, which is realised with the concurrence of public and private subjects, i.e., operators and broadcasters. Private parties are thus fully and legitimately recognised as providers of radio and television services, under Articles 21 and 41 of the Constitution, on the free expression of thought and free economic initiative. The Constitutional Court had previously expressed itself very clearly in ruling No. 826/1988 in the name of the freedom of expression of as many voices as possible, public and private, without any danger of marginalisation due to the concentration of technical and economic resources in the hands of one or a few. In accordance with the Mammì Law, broadcasting radio or television programmes by any technical means „is of overriding general interest" (Art. 1). The law reiterates pluralism, distinguishing it between internal and external. The internal one is an expression of „openness to different opinions, political, social, cultural and religious tendencies" (Art. 2), and the external one is „the possibility for different players to enter the market".

The content of the Mammì Law was updated by Law No. 112 of 3 May 2004, known as the Gasparri Law – referring to Maurizio Gasparri, Minister of Communications in office at the time – a proxy law that was implemented through the Consolidated Law on Television in the following year. Also, in this text, pluralism of information is safeguarded, and the subjects that constitute the governing bodies of broadcasting are reaffirmed:

1. The Ministry of Communications merged into the Ministry of Enterprise and Made in Italy, which deals with industrial policy, trade and communications. Regarding the Communications Policy, it deals with regulating electronic

[17] Cf. F. Monteleone, *Storia della radio e della televisione in Italia: Costume, società e politica*, Venezia 2013.

communications, radio and television broadcasting and the postal sector, RAI and Poste Italiane, mobile telephony and emergency services, national radio spectrum and broadband[18].

2. The Communications Guarantee Authority: in fact, it was created as an antitrust authority, with the task of guaranteeing pluralism, both in the expression within programming and in the concentration of resources and instruments. Among its tasks is the national plan for frequency assignment; communications security and electromagnetic interference; control activities of the telecommunications market in the protection of pluralism, the freedom of expression of thought, speech writing and any other means of dissemination, including the press free of authorisations and censorship. Furthermore, it protects the freedom and secrecy of communication via the internet. It preserves the security of electronic communication networks and frees economic initiatives under competition according to objectivity, transparency, non-discrimination and proportionality[19].

3. The President of the Council of Ministers uses the Presidency of the Council of Ministers to exercise autonomous functions of impulse, direction and coordination attributed to him/her by the Constitution and the laws of the Republic[20].

4. The Parliamentary Commission for the General Direction and Supervision of Radio and Television Services, composed of members of Parliament and the Senate to supervise the national and public radio and television service (Radio Televisione Italiana), defines the direction of programming, advertising and corporate economy[21].

5. Rights, fundamental freedoms, and respect for dignity when processing personal data are protected by the Garante per la Protezione dei Dati Personali (GPDP)[22].

6. The Competition Authority protects both competition and the market[23].

7. Finally, it is up to the regions to safeguard compliance with the rules on communication spaces during elections and to protect the communication

[18] www.mise.gov.it/it/ [access: 10.03.2023].

[19] www.agcom.it/ [access: 10.03.2023].

[20] www.governo.it/it [access: 10.03.2023].

[21] G.U. Rescigno, *A proposito delle convenzioni costituzionali (la nomina del presidente della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi)*, „Diritto pubblico, Rivista fondata da Andrea Orsi Battaglini" 2008, no. 3, p. 911–926.

[22] www.garanteprivacy.it/ [access: 10.03.2023].

[23] www.agcm.it/ [access: 10.03.2023].

spaces[24] – and also cultural production spaces – of linguistic minorities recognised by law[25].

8. The regional body delegated to these forms of control and protection is the Regional Communications Committee (Co.re.com), which also carries out, with regard to the local radio and television sector, supervision of the protection of minors, the publication and dissemination of polls and compliance with programming obligations[26].

Up to this point, we have outlined the structure of the Italian state in terms of public safety with reference to traditional media, but the transition from analogue to digital did not only represent a technological boundary but also a boundary between what is regulated and what is not. And although the principle of analogy was applied in filling a legal void, it did not serve to fill the cultural void and the perception of what was, or was not, a crime for citizens (from the duplication and sharing of intellectual products to personal, institutional attacks or the dissemination of sensitive information), the borders of states, in a global network, and the borders between public, private citizens' or confidential public administration data pass through computer backbones, as well as processed and ferried through platforms, in the hands of private companies, which are in many cases part of conglomerates whose turnovers, networks of interest and activities are more than several countries: in this case, national and supranational public security overlap[27].

Concerning crimes against individual people, the leading source of control is the Postal and Communications Police on crimes concerning child pornography, online and child grooming on the web, such as crimes against the person committed on the web, sexual extortion, stalking, harassment and threats on social networks, depending on the profile and seriousness it acts on direct reports from victims, third parties or autonomously on its initiative[28].

Law No. 82 of 14 June 2021 established the National Cybersecurity Agency (NCA), which promotes a coherent regulatory framework in the sector

[24] P. Caretti, *Le fonti della comunicazione*, „Quaderni costituzionali. Rivista italiana di diritto costituzionale" 2004, no. 2, p. 313–324.

[25] C. Sagone, *Lingua, minoranza e strumenti di tutela tra Stato e Regioni*, „Diritti regionali. Rivista di diritto delle autonomie territoriali" 2023, no. 1.

[26] www.agcom.it/co.re.com [access: 10.03.2023].

[27] N. Strizzolo, *Attacco informatico e mondo digitale tra prevenzione e difesa*, „Sicurezza e Scienze Sociali" 2014, no. 1, p. 38–52.

[28] N. Ciardi, *Polizia postale, tutto ciò che fa per proteggerci su internet*, www.agendadigitale.eu/sicurezza/polizia-postale-cio-proteggerci-internet/ [access: 10.03.2023].

and exercises inspection and sanctioning functions. It develops collaborations at the international level with counterpart agencies. It ensures coordination between public actors and public-private actions to ensure cybersecurity and cyberresilience for the country's digital development. The NCA supports national public and private actors in preventing and intervening in incidents, with the aim of promoting the national and European digital strategic autonomy in synergy with the world of production and research. It also supports training and awareness-raising in cybersecurity[29]. The philosophy guiding the NCA is to ensure the economic prosperity and security of the country during the digital transition in preventing and resolving the possible cyberattacks, and also to increase Italian independence from non-European technologies.

For national cybersecurity statistics, we can draw information directly from the „2022 Activity Report of the Postal and Communications Police and Cybersecurity Operations Centres", published on 1 March 2023[30].

In 2022, they increased:

– by three percent – the number of people and sites investigated for child pornography and online grooming;

– 178 percent more attacks on critical infrastructures of institutions, companies and individuals (increase linked to the geopolitically very critical moment);

– by 58 percent – the amounts stolen online (from EUR 73 245 740 in 2021 to 115 457 921 in 2022).

Conclusion

The issue that has emerged, mainly regarding cybercrime, is the crossing of legislative borders to countries where what is prosecutable in one state is not in another[31], and also the fact that an attack can simultaneously occur from unlimited devices that have been hacked in turn, and can spread across the network itself, even globally, as the viruses used to slow down the Iranian

[29] www.acn.gov.it/ [access: 10.09.2023].

[30] *Resoconto attività 2022 della Polizia Postale e delle Comunicazioni e dei Centri Operativi Sicurezza Cibernetica*, www.commissariatodips.it/notizie/articolo/resoconto-attivita-2022-della-polizia-postale-e-delle-comunicazioni-e-dei-centri-operativi-sicurezz/index.html [access: 10.09.2013].

[31] N. Strizzolo, *Criminalità informatica* [in:] *La devianza come sociologia*, ed. C. Cipolla, Milano 2012.

nuclear programme have created quite a few problems spreading through Western installations[32]. Furthermore, the functioning of metropolises and densely populated areas, as well as the very survival of their inhabitants, depends on supplies, logistics and facilities regulated by digital systems that are potentially vulnerable to cyberattacks.

The multi-territoriality and multi-dimensionality of the problem, which is, in fact, reducible to a single code – the digital code of machines – can turn civilisation into a great tower of Babel[33], under the threat of multiple attacks that undermine public safety and threaten people's lives.

Cybersecurity as a category aimed at strengthening public security remains present in both media systems discussed in this article. However, specific definitions, meanings and regulations are governed by individual cultural, historical and legislative considerations – hence, the evident terminological heterogeneity and focus on subjects pertinent to specific national needs. As the digitisation of social processes continues to accelerate (due to the pandemic, among other factors), rising cybersecurity threats are drawing the attention of national research centres and authorities at central, regional and local levels. It is clear that the transnational nature of cybersecurity will continue to require a multidimensional and multidisciplinary approach – one recognising both the national culture of cyberspace use and the challenges faced by the global community of cyberspace users. That is why a security organisation is needed to unite states in excellent common defence against a shared risk: like never before, Poland and Italy, too, must consider themselves neighbours.

Based on domestic regulations and programming documents, it can be concluded that Polish and Italian media systems share a similar tendency to assign the media – especially public media – with the mission of safeguarding public security through information, dedicated programming and public campaigns launched on their own or in cooperation with competent institutions and ministries. Due to the specific nature of national media systems, broadcasters address challenges embedded in domestic and regional policies. However, Polish and Italian media systems share a core dedication to universal problems (cybersecurity hygiene, prevention, rules of cyberculture) springing from the global character of cyberspace and thus warranting cooperation between national systems and transnational regulations.

[32] Eadem, *Attacco informatico...*

[33] Ibidem.

Bibliography

Bernays E.L., *Propaganda*, New York 1928.

Caretti P., *Le fonti della comunicazione*, „Quaderni costituzionali. Rivista italiana di diritto costituzionale" 2004, no. 2.

Castells M., *Władza komunikacji*, Warszawa 2013.

Garilli A., *La sicurezza sociale degli immigrati: alla ricerca della solidarietà perduta*, Bologna 2020.

Garlicki J., Noga-Bogomilski A., *Kultura polityczna w społeczeństwie demokratycznym*, Warszawa 2004.

Gierszewski J., *Bezpieczeństwo społeczne jako dziedzina bezpieczeństwa narodowego*, „Historia i Polityka" 2018, no. 23.

Kamińska-Szmaj I., *Co to jest kultura polityczna?* [in:] *Język a kultura*, vol. 11, *Język polityki a współczesna kultura polityczna*, eds. J. Anusewicz, B. Siciński, Wrocław 1994.

Karpiuk M., Makuch A., Soler U., *The Role of the Cybersecurity Strategy of the Republic of Poland in Ensuring Cybersecurity*, „Polish Political Science Yearbook" 2023, nr. 3.

Lamentowicz W., *Państwo współczesne*, Warszawa 1993.

Mazur M., *Homeostaza społeczna* [in:] *Procesy samoregulacji w oświacie. Problemy homeostazy społecznej*, eds.. M. Pęcherski, J. Tudrej, Warszawa 1983.

Monteleone F., *Storia della radio e della televisione in Italia: Costume, società e politica*, Venezia 2013.

Nye J.S. Jr, *Soft Power: The Means to Success in World Politics*, New York 2002.

Rescigno G.U., *A proposito delle convenzioni costituzionali (la nomina del presidente della Commissione parlamentare per l'indirizzo generale e la vigilanza dei servizi radiotelevisivi)*, „Diritto pubblico, Rivista fondata da Andrea Orsi Battaglini" 2008, no. 3.

Ross Ashby W., *Design for a brain. The origin of adaptative behaviour*, New York 1960.

Sagone C., *Lingua, minoranza e strumenti di tutela tra Stato e Regioni*, „Diritti regionali. Rivista di diritto delle autonomie territoriali" 2023, no. 1.

Strizzolo N., *Attacco informatico e mondo digitale tra prevenzione e difesa*, „Sicurezza e Scienze Sociali" 2014, no. 1.

Strizzolo N., *Criminalità informatica* [in:] *La devianza come sociologia*, ed. C. Cipolla, Milano 2012.

Społeczny wymiar cyberbezpieczeństwa w publicznych mediach w Polsce i we Włoszech

Streszczenie

W niniejszym artykule zbadano sposoby realizacji społecznego wymiaru bezpieczeństwa przez nadawców publicznych w Polsce i Włoszech. Nadawcy publiczni są zobowiązani do planowania i tworzenia treści zgodnie z zasadą dobra wspólnego. Jest to wymóg wynikający z krajowych przepisów dotyczących bezpieczeństwa państwa. Z perspektywy systemów krajowych o tak różnych polityczno-prawnych systemach jak Polska i Włochy można stwierdzić, że kształtowanie przestrzeni społecznej przez nadawców publicznych cechuje się podobnym pod względem strategii i taktyki kierunkiem działań.

Słowa kluczowe: system medialny, cyberbezpieczeństwo, bezpieczeństwo społeczne, stosunki międzynarodowe, współpraca międzynarodowa