Katarzyna Badźmirowska-Masłowska*

Child protection in cyberspace

Abstract

The aim of this article is to review main issues connected with the protection of a child in the cyberspace. It indicates the issue of the scientific discourse within the key terms: cyberspace and security of an underage in the online and offline environment. In the context of his position as mass media recipient and an user of cyberspace, several threats have been indicated and allocated to two basic categories: of macro-social and individual character. Premises shaping the systems of child's security in the cyberspace have been indicated and the use of legal instruments and alternative methods in terms of specific security threats has been noted. Ultimately, current challenges to increase the effectiveness of providing security in the cyberspace for an underage were formulated.

Key words: security, protection, child, underage, threat, the media

* Dr Katarzyna Badźmirowska-Masłowska, Instytut Prawa, Wydział Bezpieczeństwa Narodowego, Akademia Sztuki Wojennej w Warszawie, e-mail: k.badzmirowskam@gmail.com.

Introduction

Child protection[1] in cyberspace, understood in the informative context of its kind[2], is a complex subject of consideration of almost all fields and many scientific disciplines[3], setting the framework for systemic (ergo containing complementary instruments of hard and soft law and alternative measures) protection of a juvenile. This implies a number of controversies, in particular, regarding fundamental terminological issues, i.e. a child or cyberspace, i.e. the subject and the ecosystem of its daily functioning.

The very definition of "a child", traditionally meaning in the context of Article 1 of the Convention on the Rights of the Child of November 11, 1989[4] any human being under 18 years of age is not precise enough to properly address the subject issues. First of all, for the audio-visual sector, and more broadly - the space determined by the development of information and communication technologies (ICT), "a child" is determined both at the international/ supranational level, covering in its scope various categories of children and young people (referred to as *a child*, *children*, *minors*, *adolescents*, *youth*, *young people*); at the national level, on the other hand, more detailed solutions are provided from the point of view of protecting safety of individual age groups against standardized types of threats, taking into account internal regulations defining the concepts of a minor, an underage or a juvenile and an adolescent. It is also necessary to take into account different - and determined in a simplified way – passive status of the recipient in linear audio-visual services and the user in the online environment[5], determining the roles a child can fulfil- a participant presenting specific behaviours, an actor (player), shaping interpersonal

1 Pojęcia dziecko i małoletni używa się w tej pracy zamiennie.

2 Por. K. Badźmirowska-Masłowska, *Małoletni użytkownik internetu a zagrożenia bezpieczeństwa informacji* [w:] W. Kitler, J. Taczkowska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017, s. 318–333.

3 Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r., w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

4 Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. nr 120, poz. 526).

5 Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L95, s. 1); por. też rewizję dyrektywy z dnia 6 listopada 2018 r.

relations and contents creator, even if it violates the regulations of the law, including criminal law or becoming a victim (an injured or harmed person). It should also be emphasized that the picture of threats should be perceived more broadly and in a more diverse way than in the case of adults, which is due to the fact that the subject of protection in the ecosystem in question is not a child in se, but the regularity of its psychophysical, socio-cultural and moral development. Furthermore, it means that child's social maladjustment should also be analysed in this respect.

Child's protection in cyberspace. Dilemmas with definitions

The concept of cyberspace which is derived from the classic novel of cyberpunk – as a variation of science fiction[6], although widely accepted in the language of the law and the lawyers, not only has it not been unequivocally accepted at the international/ supranational[7] or national level[8] of the legal definitions, but it is not sufficient for considerations regarding the safety of the juvenile

6 Por. W. Gibson, Neuromancer, P.W. Cholewa (tłum.), *Książnica*, Katowice 2009, s. 59; notabene odwołuje się ono do cybernetycznych koncepcji łączenia świata zwierzęcego (ludzkiego) i maszyn, N. Wiener, *Cybernetics: or Control and Communication in the Animal and the Machine*, Nowy Jork 1948.

7 Najwięcej wątpliwości pojawia się wokół kwestii związanych z regulacją i jurysdykcją sfery internetowej. Na forum międzynarodowym i w poszczególnych państwach toczą się debaty nad zagadnieniami związanymi z implikacjami politycznymi, ekonomicznymi oraz społeczno-kulturowymi jej rozwoju w kontekście potrzeby, ale też i możliwości efektywnej jej regulacji, w szczególności odnoszącej się do zawartości. Kwestia ta budzi kontrowersje nie tylko na europejskim poziomie regionalnym, ale także w perspektywie globalnej (por. kontrowersje wokół Communications Decency Act, np. R. Cannon, *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, „Law Journal" 1996, nr 1, s. 51–59). Z jednej strony podtrzymywane są zatem koncepcje stojące u podstaw charakterystyki ogólnoświatowej sieci jako teoretycznie nieinwigilowanej przestrzeni przepływu informacji i zawiadywanej dotychczas przez The Internet Corporation for Assigned Names and Numbers (ICANN – por. E. Salomon, K. Pijl, Applications to ICANN for Community based New Generic Top Level Domains (gTLDs): Opportunities and challenges from ahuman rights perspective, Council of Europe report, DGI(2016)17), z drugiej zaś obserwuje się inicjatywy na rzecz objęcia internetu międzynarodowymi i krajowymi regulacjami prawnymi, co z kolei budzi obawy przed jego upolitycznieniem i poddaniem pod zarząd International Telecommunication Union (ITU). RE iUE prezentują stanowisko pośrednie, np. M. Kenig-Witkowska, *Niektóre zagadnienia prawno-międzynarodowej regulacji Internetu*, „Państwo i Prawo" 2001, z. 9, s. 58 i nast.; por. też uwagi ITU (Internet Policy and Governance), online.

8 Por. definicję odpowiadającą zasadniczo technologicznemu punktowi widzenia, zawartą w ustawie z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz

in the overlapping dimensions of offline and online life[9]; the technological, information and political and economic perspectives should be supplemented by the socio-cultural aspects of the virtual communication[10], which is not unreal, although existing in experience detached from direct and creating other forms of socialization[11]. The new cultural paradigm is embedded in an approach sometimes opposing the technological determinism of the constructivist concept[12], while it seems more justified to consider the network formula as part of technology of its incorporation into the everyday lives of individuals and society rather than being separate and parallel to reality[13]; virtual reality is a process through which the information society expresses itself[14] .

o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. nr 222, poz. 1323).

9 W zmediatyzowanych społeczeństwach zacierają się granice między rzeczywistym życiem a jego wirtualnym obrazem; S. Lash, J. Urry, *Postmodernist Sensibility* [w:] A. Giddens, D. Held, S. Loyal, D. Seymour, J. Thompson (red.), *The Polity Reader in Cultural Theory*, Cambridge 1994, s. 135. Wobec potrzeby łącznego postrzegania rzeczywistości realnej i wirtualnej dyskusje dotyczą też koncepcji autonomizacji cyberkultury prawnej, por. K. Dobrzeniecki, *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?* [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008, s. 316 i nast.; J. Janowski, *Globalna cyberkultura polityki i prawa* [w:] M. Maciejewski, M. Marszał, M. Sadowski (red.), *Tendencje rozwojowe myśli politycznej i prawnej*, Wrocław 2014, s. 311–325.

10 Por. D. de Kerckhove, *Inteligencja otwarta. Narodziny społeczeństwa sieciowego*, online; M. Szpunar, *Przestrzeń internetu – nowy wymiar przestrzeni społecznej* [w:] A. Siwik, I. Haber (red.), *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, Kraków 2008, s. 225–234 (i cytowana tam literatura). Przy czym niezasadne jest ani zbyt wąskie utożsamianie cyberprzestrzeni z technologicznym pojęciem internetu, ani z nadmiernie upraszczającą synonimizacją jej ze sferą wirtualną, J. Kulesza, *Międzynarodowe prawo Internetu*, Poznań 2010, s. 57; M. Ostrowicki, *Wirtualne realis. Estetyka w epoce elektroniki*, Kraków 2006, s. 119 i nast.

11 Należy rozważyć, że w istocie rzeczywistość, której człowiek doświadcza, jest zawsze wirtualna, bowiem postrzegana jest właśnie przez symbole, K. Krzysztofek, *Zmiana permanentna? Refleksje o zmianie społecznej w epoce technologii cyfrowych*, „Studia Socjologiczne" 2012, nr 4, s. 9.

12 Por. np.: M. Szpunar, *Nowe-stare medium. Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego*, Warszawa 2012, pkt 1.4, *Konstruktywizm versus technologiczny determinizm*, s. 33–44.

13 Por. np.: M. Castells, *Społeczeństwo sieci*, M. Marody, K. Pawluś, J. Stawiński, S. Szymański (tłum.), Warszawa 2010, s. 46–47; T. Goban-Klas, *Społeczeństwo medialne*, Warszawa 2005, s. 165 i nast.; M. Gruchoła, *Nowe formy zachowań społecznych wobec i pod wpływem mediów oraz nowych technologii. Analizy porównawcze*, „Państwo i Społeczeństwo" 2017, nr 3, s. 12 i nast.

14 R.W. Kluszczyński, *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów*, Kraków 2001, s. 80; Globalne Społeczeństwo Informacyjne (GSI) za: P. Sienkiewicz, H. Świeboda, *Ewaluacja strategii rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe. Ekonomiczne Problemy Usług" 2010, nr 57; *E-gospodarka w Polsce. Stan obecny i perspektywy rozwoju*,

The impact of ICT is most strongly observed in the category of a juvenile, for whom they become an integral and important part of life, *ergo* the intensity of social change is associated here with particular vulnerability to their impact, especially in the conditions of replacement of national and regional cultures with global patterns; especially since contemporary, individual mass media are now entering the area traditionally affected by primary structures, such as family, school, and friends. To consider the title issues, the concept of cyberspace, adopted in the legal regulations, doctrine and jurisprudence, needs to be supplemented with the perspective of other scientific disciplines dealing with communication issues (science of social communication and media, sociology, psychology, pedagogy, security science, but also linguistics, philosophy, telecommunications)[15].

In the light of the revolutionary pace of changes in the overall life of modern societies and individuals creating them, caused by the rapid development of ICT, the perception of the safety of a juvenile in the information and its social context also undergoes transformation. Apart from the need to use broader than negative approaches to security, it is crucial to categorize threats (*risks*, *dangers*, *threats*) in the paradigm of macro-social preponderance or an individual perspective of their consideration[16].

In the first category, attention deserve the following negative effects: 1) digital exclusion; 2) global, uniformed cultural patterns, often in opposition to the axiological systems of communities traditionally adopted in a given region; 3) concentration around consumer and mercantile values, changing especially the concepts of privacy and security in the economic area.

In the second category, however: 1) sexual crime against a child; 2) the content traditionally considered harmful to the development of a juvenile recipient (pornography and violence); 3) technologically implied transformations of traditional threats (cyberthreats), deciding on their

cz. I, Szczecin 2010, s. 132; P. Sienkiewicz, *Teoria rozwoju społeczeństwa informacyjnego* [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, Kraków 2002, s. 506–507.

15 Zagadnienie wymaga szerszego, odrębnego opracowania; tu wskazano jedynie główne aspekty podlegające dyskusji.

16 Por. K. Badźmirowska-Masłowska, *Zagrożenia dla małoletniego ze strony mediów audiowizualnych. W kierunku nowego paradygmatu?* [w:] M. Szymczyk, R. Grzywacz (red.), *W trosce o człowieka. Paradygmaty stare i nowe*, Kraków 2016, s. 239–250.

intensity and increase in the scope (e.g. *cyberbullying*); 4) hazards specific to online environment (e.g. addictions).

The threats in question affect the following sphere: sexual (erotic), aggression, values, and relate both to the status of the child as a recipient of mass media, as well as the participant, actor and creator of their network types. Despite the fact that the juvenile comes into contact with a wide spectrum of these dangers, one should bear in mind that the very risk of their occurrence does not mean automatic damage, but it is rather its probability that is estimated, especially since the network ecosystem creates a kind of a dual space called risky opportunities, on the one hand conducive to the child's development, and on the other, exposing the child to unprecedented dangers[17]. Vulnerability of a juveniles shaped at the macro-social and individual level, in a way in opposition to the ability to deal effectively with them, to respond to them in a balanced way (*resilience*) and to constructively cope with them (*cope*), determined by their awareness, psychophysical fitness and social, knowledge and skills, *ergo* media competence[18]; the individual paradigm created by the above conditions the adopted methods of protecting a minor in cyberspace.

Methods of protecting a juvenile in cyberspace

The purpose of protecting a child in cyberspace is, on the one hand, to ensure the child's safety and, on the other, to ensure proper conditions of the child's development. Referring to the aspect of counteracting threats, nota bene, usually perceived analogically to the offline sphere and in accordance with the principle of technological neutrality[19], one should indicate the need for its systemic shaping, based on its *multi-layered*, encompassing many stakeholders and multi-level (*multi-level*) approach[20].

17 18 Por. np. recommendation of the OECD The protection of children online, 2012; OECD Council report on risks faced by children online and policies to protect them, 2012, online, szerzej, por. np.: K. Badźmirowska-Masłowska, *Protecting minors from internet threats. Legal instruments or alternative measures?* [w:] M. Sitek, A.F. Uricchio, I. Florek (red.), *Human Rigts, between needs and possibilities*, Józefów 2017, s. 35–58 (i cytowana tam literatura).

18 Ibidem.

19 Por. np.: N. van Eijk, *Net Neutrality and Audiovisual Services*, „Iris plus" 2011, nr 5, s. 7–19.

20 OECD Report on risks faced by children online and policies to protect them has indicated the various dimensions of child protection policy: multi-layered, multi-stakeholder and multi-level..., s. 40–49.

The first component contains direct and indirect tools that combine legal instruments with alternative methods.

The category of the stakeholders covers a wide range of obligation sharing recipients, from the representatives of public authorities (especially relevant ministers of education, culture, health, justice, etc.), the representatives of business (media, telecommunications, etc.) to the information society (civil, e.g. in the form of NGOs); special attention should be given to parents/guardians, school or broadly understood educational environment.

What is important, it is indicated that the objectives of the protection in question should be adopted, within the framework of regional standards (here European), at the governmental level, which allows monitoring their implementation, proposing new initiatives, establishing and conducting cooperation within national and international (transnational) and finally promotes cooperation between the private (commercial) and non-governmental sectors. Multilevel politics means conducting it both at the state level and - on the basis of cooperation – at the international level, while in the case of the European continent both the Council of Europe and the European Union constitute in this respect regional standards of soft or hard law, depending on the type of threat. Harmonization of regulations and cooperation within programs, due to the cross-border nature of cyberspace, is a necessary condition for the effectiveness of national security systems.

When considering the basic premises for choosing legal or alternative methods of protecting a minor, the following should be indicated: 1) seriousness of the threat – constituting a crime or other disruption to the correct development of the child, with sexual offenses directed against him defined as particularly harmful[21]; 2) technical aspects of access to dangerous content, contacts and behaviour – depending on the type of audio-visual service (linear or on demand) or other service provided by the internet (especially individual mass media); 3) extent of a given threat – determining both the macro-social or individual nature of it and the need for an internal or international level of response; 4) the age category of children and youth- setting protection measures appropriate to the minor's development level (both in technical and social terms). According to the aforementioned premises, different types of legal

21 Overall, legislation pertaining to all illegal content is applying across all offline and online media and it is predominantly regulated on national level within the scope of general laws (e.g. consumer or privacy and information security related risks for minors), K. Badźmirowska-Masłowska, *Protecting*..., s. 45.

instruments and alternative measures are applied to the identified types of threats. In general[22], criminal law instruments are mainly used in the area of sexual crime against the child[23]; they specify which deeds should be criminalised, the amount of the minimum maximum penalties and raise the issue of the age of relevant consent to sexual activities. As regards procedural guarantees, the states are required to: ensure the conditions for reporting suspected sexual abuse or child sexual exploitation (art. 16 of Directive 2011/92/EU), assistance and support to minors who are the victims of crime before the commencement of preparatory proceedings, during its duration, as well as during legal proceedings (victims, art. 18–20 of the above-mentioned directives and Article 31–36 of the Lanzarote Convention). Furthermore, they should introduce preventive intervention programs or measures (art. 21–25 of the beforementioned directive and Article 4–17 of the Lanzarote convention).

Alternative methods are of particular importance to ensure child's protection in the online environment. In particular, the following are worth mentioning: 1) self and coregulation arising from the bottom up, as well as at the initiative of the regulating bodies[24]; 2) technical measures – restricting access, but also marking content[25]; 3) methods for strengthening awareness of threats – based on education or social (information) campaigns[26];

22 Szersze omówienie zagadnienia przekracza ramy tego opracowania.

23 Por. Konwencję Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych, sporządzoną w Lanzarote dnia 25 października 2007 r., Dz.U. z 2015 r., poz. 608 oraz dyrektywę Parlamentu Europejskiego i Rady 2011/92/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępująca decyzję ramową Rady 2004/68/WsiSW, Dz.Urz. UE L 335, s. 1–14; szerzej, np.: K. Badźmirowska-Masłowska, *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investment in the Common future*, Olsztyn 2013, s. 147–160. Instrumenty prawne stosuje się także względem innych zagadnień, związanych np. z naruszeniami prywatności, por. np.: K. Badźmirowska-Masłowska, *Wizerunek dziecka w internecie a zagrożenia prawa do prywatności* [w:] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017, s. 49–61.

24 Por. np. recommendation REC (2001)8 of the Committee of Ministers to member states on Self-regulation concerning cyber content.

25 Por. np. recommendation CM/Rec(2008)6 of the Committee of Ministers to member states on measures to promote the respect for freedom of expression and information with regard to internet filters.

26 Por. np. recommendation 1586 (2002) The digital divide and education; recommendation orazRec(2006)12 of the Committee of Ministers to member states on empowering children in the new information and communications environment.

4) other – program-based assistance points, *so-called hot lines (helplines*, insafe, inhope)[27] or creating *child protection zones*[28].

Support may come from various stakeholder groups initiating actions at the national and international level for the implementation of children's rights[29]; the most well-known program here is Better Internet for Kids[30], and the research space – EU Kids Online[31].

Summary

When considering the issues of child protection in cyberspace, conclusions should be presented regarding initiatives and actions that should be raised to increase its effectiveness. The first issue is conducting extensive research in the field of: 1) terminological arrangements as to the concept of: 1) cyberspace – as an environment for the functioning of a minor, equal to offline reality, together with the determination of the interrelationship between both dimensions of its life; 2) the status of the child - as the recipient of audio-visual media and other audio-visual network services, in the context of being recognized as an object of protection for its proper development; 3) security – as an aspect of research on these issues; 2) changes in the role of audio-visual media, and more broadly the virtual / internet / cyberspace environment – as to the strength and scope of their impact on contemporary generations of children and youth.

The research above should be focused on creating a national strategy for the protection of a minor. It should be based on the pillars of the EU Safer Internet Strategy[32], which relates to: 1) publishing high-quality content (creative, educational) online for children and young people and promoting positive online experiences for children; 2) increasing awareness, especially

27 Online.
28 Np. online.
29 Global Alliance against Child Sexual Abuse Online, 2015 Threat AssesmentReoport, online.
30 Por. też: K. Badźmirowska-Masłowska, *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci*, „Journal of Modern Science" 2012, nr 3, s. 433–472.
31 Online.
32 Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów, Europejska strategia na rzecz lepszego internetu dla dzieci, COM(2012) 196 final.

of end users (parents / guardians, minors themselves etc.) and strengthening rights, shaping digital skills and using the media, including the introduction of online safety education in school programs and expanding information activities (e.g. campaigns) and enabling reporting of violations of law and security; 3) creating a safe online ecosystem for the juvenile by adapting privacy and advertising settings to age, popularizing the use of parental control tools, widespread use of age ratings and content classification; 4) combating sexual crime against a child in international cooperation through faster and systematic identification of materials depicting such acts. Both at the international (universal, regional, supranational) and national levels, a number of initiatives are observed focused on child protection in cyberspace and involving entities from the public, private and non-governmental sector. However, the analysis of the situation in Poland indicates that the already existing wide interaction of recipients of obligations, fulfilling the areas of prevention and combating undesirable effects, requires the development of appropriate procedures or mechanisms for coherent cooperation; therefore, the need to create a strategy for the protection of a minor in cyberspace, taking into account the penetration of offline and online worlds in everyday life as a fundamental premise, should be considered urgent. It should include legal instruments and alternative measures in a complementary manner, with particular emphasis on the issues of social education and systemic cooperation of stakeholders representing different categories; it should also resolve counteraction to which threats requires particularly intense cooperation at the international – regional/supranational or even universal level.

Bibliography

Literature

Badźmirowska-Masłowska K., *Edukacyjne aspekty bezpieczeństwa nowych technologii komunikacyjnych dla małoletnich w świetle Strategii Unii Europejskiej na rzecz lepszego Internetu dla dzieci*, „Journal of Modern Science" 2012, nr 3.

Badźmirowska-Masłowska K., *Fighting against child sexual abuse and child sexual exploitation in Europe. Media and internet perspective* [w:] M. Sitek, G. Dammacco, A. Ukleja, M. Wójcicka (red.), *Europe of Founding Fathers. Investment in the Common future*, Olsztyn 2013.

Badźmirowska-Masłowska K., *Małoletni użytkownik internetu a zagrożenia bezpieczeństwa informacji* [w:] W. Kitler, J. Taczkowska (red.), *Bezpieczeństwo informacyjne. Aspekty prawno-administracyjne*, Warszawa 2017.

Badźmirowska-Masłowska K., *Protecting minors from internet threats. Legal instruments or alternative measures?* [w:] M. Sitek, A.F. Uricchio, I. Florek (red.), *Human Rigts, between needs and possibilities*, Józefów 2017.

Badźmirowska-Masłowska K., *Wizerunek dziecka w Internecie a zagrożenia prawa do prywatności* [w:] K. Chałubińska-Jentkiewicz, K. Kakareko, J. Sobczak (red.), *Prawo do prywatności jako reguła społeczeństwa informacyjnego*, Warszawa 2017.
Badźmirowska-Masłowska K., *Zagrożenia dla małoletniego ze strony mediów audiowizualnych. W kierunku nowego paradygmatu?* [w:] M. Szymczyk, R. Grzywacz (red.), *W trosce o człowieka. Paradygmaty stare i nowe*, Kraków 2016.
Cannon R., *The Legislative History of Senator Exon's Communications Decency Act: Regulating Barbarians on the Information Superhighway*, „Law Journal" 1996, nr 1.
Dobrzeniecki K., *Autonomiczne prawo cyberprzestrzeni: mit czy rzeczywistość?* [w:] O. Bogucki, S. Czepita (red.), *System prawny a porządek prawny*, Szczecin 2008.
Goban-Klas T., *Społeczeństwo medialne*, Warszawa 2005.
Gruchoła M., *Nowe formy zachowań społecznych wobec i pod wpływem mediów oraz nowych technologii. Analizy porównawcze*, „Państwo i Społeczeństwo" 2017, nr 3.
Janowski J., *Globalna cyberkultura polityki i prawa* [w:] M. Maciejewski, M. Marszał, M. Sadowski (red.), *Tendencje rozwojowe myśli politycznej i prawnej*, Wrocław 2014.
Kenig-Witkowska M., *Niektóre zagadnienia prawno-międzynarodowej regulacji Internetu*, „Państwo i Prawo" 2001, z. 9.
Kluszczyński R.W., *Społeczeństwo informacyjne. Cyberkultura. Sztuka multimediów*, Kraków 2001.
Krzysztofek K., *Zmiana permanentna? Refleksje o zmianie społecznej w epoce technologii cyfrowych*, „Studia Socjologiczne" 2012, nr 4.
Kulesza J., *Międzynarodowe prawo Internetu*, Poznań 2010.
Lash S., Urry J., *Postmodernist Sensibility* [w:] A. Giddens, D. Held, S. Loyal, D. Seymour, J. Thompson (red.), *The Polity Reader in Cultural Theory*, Cambridge 1994.
Ostrowicki M., *Wirtualne realis. Estetyka w epoce elektroniki*, Kraków 2006.
Sienkiewicz P., Świeboda H., *Ewaluacja strategii rozwoju społeczeństwa informacyjnego*, „Zeszyty Naukowe. Ekonomiczne Problemy Usług" 2010, nr 57.
Sienkiewicz P., *Teoria rozwoju społeczeństwa informacyjnego* [w:] L.H. Haber (red.), *Polskie doświadczenia w kształtowaniu społeczeństwa informacyjnego. Dylematy cywilizacyjno-kulturowe*, Kraków 2002.
Szpunar M., *Nowe-stare medium. Internet między tworzeniem nowych modeli komunikacyjnych a reprodukowaniem schematów komunikowania masowego*, Warszawa 2012.
Szpunar M., *Przestrzeń internetu – nowy wymiar przestrzeni społecznej* [w:] A. Siwik, I. Haber (red.), *Od robotnika do internauty. W kierunku społeczeństwa informacyjnego*, Kraków 2008.
Wiener N., *Cybernetics: or Control and Communication in the Animal and the Machine*, Nowy Jork 1948.

Legal acts

Konwencja o prawach dziecka z dnia 20 listopada 1989 r. (Dz.U. z 1991 r. nr 120, poz. 526).
Dyrektywa Parlamentu Europejskiego i Rady 2010/13/UE z dnia 10 marca 2010 r. w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych państw członkowskich dotyczących świadczenia audiowizualnych usług medialnych (dyrektywa o audiowizualnych usługach medialnych) (Dz.Urz. UE L95, s. 1).
Ustawa z dnia 30 sierpnia 2011 r. o zmianie ustawy o stanie wojennym oraz o kompetencjach Naczelnego Dowódcy Sił Zbrojnych i zasadach jego podległości konstytucyjnym organom Rzeczypospolitej Polskiej oraz niektórych innych ustaw (Dz.U. nr 222, poz. 1323).
Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 20 września 2018 r., w sprawie dziedzin nauki i dyscyplin naukowych oraz dyscyplin artystycznych (Dz.U. z 2018 r., poz. 1818).

Ochrona dziecka w cyberprzestrzeni

Streszczenie

Celem artykułu jest przegląd głównych zagadnień, łączących się z ochroną dziecka w cyberprzestrzeni. Wskazuje on na problematykę dyskursu naukowego w obrębie kluczowych pojęć, tj. cyberprzestrzeń i bezpieczeństwo małoletniego w środowisku *on-line* i *off-line*. W kontekście jego pozycji jako odbiorcy mass mediów i użytkownika cyberprzestrzeni, stypizowano poszczególne zagrożenia, przyporządkowując je dwóm podstawowym kategoriom: o charakterze makrospołecznym i indywidualnym. Wskazano na przesłanki kształtujące systemy ochrony dziecka w cyberprzestrzeni oraz zasygnalizowano stosowanie instrumentów prawnych i metod alternatywnych względem konkretnych zagrożeń. Finalnie sformułowano aktualne wyzwania dla zwiększenia efektywności zapewnienia małoletniemu bezpieczeństwa w cyberprzestrzeni.

Słowa kluczowe: bezpieczeństwo, ochrona, dziecko, małoletni, zagrożenie, media