Elżbieta Cygnar[1]
Akademia Nauk Stosowanych w Nowym Sączu
Agata Bubenko[2]
Sławomir Żurawski[3]
Uniwersytet Andrzeja Frycza Modrzewskiego w Krakowie

https://doi.org/10.29316/9788368103373_19

CYBERBEZPIECZEŃSTWO DZIECI I MŁODZIEŻY W DOBIE WSPÓŁCZESNYCH ZAGROŻEŃ

CYBERSECURITY FOR CHILDREN AND YOUNG PEOPLE IN THE AGE OF MODERN THREATS

Streszczenie

Celem rozdziału jest przedstawienie i omówienie współczesnych wyzwań dotyczących ochrony dzieci i młodzieży w środowisku cyfrowym. W pierwszej części rozdziału omówiono istotę cyberprzestrzeni jako nowego środowiska życia, nauki i rozwoju dzieci oraz młodzieży. Autorzy analizują definicje pojęcia „cyberprzestrzeń", wskazując na jej dynamiczny, interaktywny i wirtualny charakter, który w znacznym stopniu wpływa na sposób komunikacji i funkcjonowania młodego pokolenia. W kolejnej części opisano główne zagrożenia, na jakie narażone są dzieci i młodzież w cyberprzestrzeni. Zjawiska te zostały poparte wynikami badań i raportów

[1] https://orcid.org/0009-0004-5377-9588, e-mail: ecygnar@ans-ns.edu.pl
[2] https://orcid.org/0009-0005-3152-9884
[3] https://orcid.org/0000-0001-9527-3391, e-mail: slawomir.zurawski@onet,pl

międzynarodowych instytucji, takich jak NASK, EU Kids Online, WHO czy Europol. Następna część rozdziału poświęcona została analizie aspektów prawnych i instytucjonalnych związanych z ochroną dzieci w sieci. Problem badawczy został sformułowany w następujący sposób: w jaki sposób można skutecznie chronić dzieci i młodzież przed współczesnymi zagrożeniami w cyberprzestrzeni? Przyjęta hipoteza badawcza zakłada, że skuteczna ochrona najmłodszych użytkowników Internetu wymaga zintegrowanego podejścia, łączącego działania edukacyjne, profilaktyczne i prawne z rozwijaniem kompetencji cyfrowych oraz współpracą szkoły, rodziny i instytucji publicznych. W ramach metodyki badań wykorzystano analizę literatury przedmiotu, aktów prawnych, raportów instytucji zajmujących się bezpieczeństwem cyfrowym, a także analizę porównawczą wybranych programów edukacyjnych realizowanych w Polsce i na świecie. Z przeprowadzonej analizy wynika, że ochrona dzieci i młodzieży w środowisku cyfrowym wymaga podejścia interdyscyplinarnego, łączącego wiedzę z zakresu pedagogiki, psychologii, technologii informacyjnych i prawa. Kluczową rolę odgrywają edukacja cyfrowa, rozwijanie świadomości zagrożeń, kształtowanie odpowiedzialnych postaw wśród uczniów, rodziców i nauczycieli oraz budowanie empatii i odpowiedzialności w kontaktach online.

Słowa kluczowe: cyberbezpieczeństwo, dzieci i młodzież, cyberprzemoc, edukacja cyfrowa, ochrona prawna

Abstract

The aim of the article is to present and discuss contemporary challenges regarding the protection of children and young people in the digital environment. The first part of the article presents the essence of cyberspace as a new environment for the living, learning and development of children and young people. The authors analyse the definitions of the term “cyberspace”, highlighting its dynamic, interactive, and virtual character, which significantly affects how the younger generation communicates and functions. The next part describes the main threats to which children and young people are exposed in cyberspace. Each of these phenomena has been supported by research findings and reports from international institutions such as NASK, EU Kids Online, WHO, and Europol. The next part of the article analyses the legal and institutional aspects of protecting children online. The research problem was formulated in: how can children and young people be effectively protected from modern threats in cyberspace? The adopted research hypothesis assumes that effective protection of the youngest Internet users requires an integrated approach, combining educational, preventive and legal activities with the development of digital competences and cooperation between the school, family and public institutions. As part of the research methodology, an analysis of the literature on the subject, legal acts, reports of institutions dealing with digital security, and a comparative analysis of selected educational programs implemented in Poland and around the world were used. The

analysis shows that protecting children and young people in the digital environment requires an interdisciplinary approach that combines knowledge from pedagogy, psychology, information technology, and law. Digital education plays a key role, developing awareness of risks, shaping responsible attitudes among students, parents and teachers, and building empathy and responsibility in online contacts.

Keywords: cybersecurity, children and young people, cyberbullying, digital education, legal protection

Wstęp

Współczesny świat rozwija się w niewyobrażalnie szybkim tempie. Szczególny wpływ ma na to stale postępujący proces globalizacji, który sprawia, iż staje się on jedną wielką informacyjną wioską. Dynamiczny rozwój technologii informacyjno-komunikacyjnych (TIK) w ostatnich dekadach w sposób zasadniczy przekształcił codzienne funkcjonowanie jednostki w społeczeństwie. Internet stał się powszechnym narzędziem komunikacji, edukacji, pracy i rozrywki, a jego dostępność sprawiła, że również dzieci i młodzież coraz częściej korzystają z zasobów cyfrowego świata. Młode pokolenie, dorastające w warunkach cyfrowej immersji, określane mianem „cyfrowych tubylców", cechuje się wysokim poziomem kompetencji technicznych, lecz nierzadko niską świadomością zagrożeń wynikających z aktywności online. Rozwój technologii informacyjno-komunikacyjnych zrewolucjonizował życie człowieka, usprawnił jego funkcjonowanie w wielu obszarach, jednakże znacząco poszerzył katalog istniejących zagrożeń. Jako że tzw. cyberprzestrzeń stała się głównym obszarem funkcjonowania dużej części społeczeństwa, istotną jest zatem kwestia wszelkich zagrożeń płynących z nieograniczonych wręcz możliwości przebywania w tejże „cyberprzestrzeni".

Wzrost obecności przede wszystkim młodych użytkowników w przestrzeni wirtualnej niesie ze sobą liczne ryzyka, takie jak cyberprzemoc, kontakt z niepożądanymi treściami, uzależnienie od mediów cyfrowych, nadużywanie mediów społecznościowych, manipulacja informacyjna czy nieuprawnione przetwarzanie danych osobowych. Problemy te mają charakter interdyscyplinarny, obejmujący aspekty psychologiczne, społeczne, pedagogiczne i prawne, co sprawia, że kwestia cyberbezpieczeństwa najmłodszych staje się jednym z kluczowych wyzwań współczesnej edukacji i polityki bezpieczeństwa informacyjnego.

Cyberprzestrzeń jako środowisko rozwoju dzieci i młodzieży

Termin „cyberprzestrzeń" pojawił się po raz pierwszy w 1984 roku w opowiadaniu „Wypalić Chrom" autorstwa pisarza *science fiction* Williama Gibsona, według którego jest to konsensusowa halucynacja doświadczana każdego dnia przez miliardy uprawnionych użytkowników, niejako graficzne odwzorowanie danych pobieranych z banków wszystkich komputerów świata. Określenie „cyberprzestrzeń" zostało przeniesione zatem z literackiej formy na kształtującą się nową rzeczywistość w świecie (Konieczniak, 2011). Pierre Lévy charakteryzuje cyberprzestrzeń jako przestrzeń możliwości otwartego komunikowania się za pośrednictwem połączonych komputerów i pamięci informatycznych pracujących na całym świecie. Podkreśla fundamentalną cechę cyberprzestrzeni, czyli jej cyfrowy charakter, który jest „plastyczny, płynny, obliczalny z dużą dokładnością i przetwarzalny w czasie rzeczywistym, hipertekstualny, interaktywny i wreszcie wirtualny" (Lévy, 2002).

Definiując cyberprzestrzeń, należy zwrócić przede wszystkim uwagę na znaczenia słów składających się na jej nazwę – cyber i przestrzeń. Bowiem termin cyber pochodzi od cybernetyki, czyli nauki o sterowaniu i komunikacji w systemach oraz przetwarzaniu informacji w tych systemach, zapoczątkowanej przez Norberta Wienera. Natomiast Margaret Mead uważa, iż: „cybernetyka – to forma interdyscyplinarnej myśli, która umożliwiła członkom różnych dyscyplin komunikację między sobą w języku zrozumiałym dla wszystkich". Zatem cyberprzestrzeń może być rozumiana jako przestrzeń komunikacji, gdzie sprzężenie zwrotne informacji pozwala na regulację systemów, wzajemne między nimi relacje, dynamiczny rozwój i wytyczanie szlaków (Konieczniak, 2011).

Cyberprzestrzeń często pojmowana jest po prostu jako rzeczywistość wirtualna, którą można wytłumaczyć, korzystając z angielskiej definicji słowa „wirtualny" – to jest: „symulowany, pełniący funkcję czegoś, co w istocie nie istnieje". Wobec powyższego, Piotr Sitarski dochodzi do stwierdzenia, że rzeczywistość wirtualna ma wszystkie cechy prawdziwego świata, oprócz jednej: istnienia (Konieczniak, 2011). Natomiast dynamika rozwoju Internetu i głębokie osadzenie współczesnego społeczeństwa w cyberprzestrzeni wskazują, iż ludzie zatracają się w tym nieprawdziwym świecie, bowiem wszystko dociera poprzez media, człowiek przenosi swoje życie do cyberprzestrzeni, a rzeczywistość realna i wirtualna przenikają się.

Zatem chyba najbardziej praktyczną definicją dla terminu „cyberprzestrzeń" jest dyrektywa 54 National Security Presidential, według której pojęcie to jest rozumiane jako wirtualne środowisko informacji i interakcji między ludźmi. Owe interakcje to bogaty zbiór odzwierciedlający zarówno pozytywne, jak i negatywne strony ludzkiej natury, wahający się od cyberautokreacji i autoekspresji do działań przestępczych prowadzących również do aktów terrorystycznych oraz możliwych konfliktów cybernetycznych. Dzieje się tak z powodu głównych cech cyberprzestrzeni, którymi są: brak granic, dynamiczne procesy i zjawiska oraz anonimowość użytkowników (Wochnowicz, 2023).

Internet jest aktualnie przestrzenią pracy i edukacji, ale również środowiskiem socjalizacji, rozrywki i samoekspresji. Zjawisko to szczególnie dotyczy dzieci i młodzieży, które dorastają w rzeczywistości cyfrowej, korzystając z technologii w sposób naturalny i intuicyjny, bowiem cyberprzestrzeń staje się miejscem, w którym młodzież kształtuje swoje relacje społeczne, tożsamość i kompetencje cyfrowe, to powoduje, że granice między światem realnym a wirtualnym stają się płynne, z zatem relacje, edukacja, rozrywka i komunikacja coraz częściej odbywają się w przestrzeni cyfrowej (Solecki, 2017). Współczesna młodzież określana jest często mianem cyfrowych tubylców (digital natives), czyli pokoleniem, które od najmłodszych lat funkcjonuje w otoczeniu technologicznym. Młodzi ludzie, to tubylcy „zamieszkali" w cyfrowym świecie. Cyberprzestrzeń stanowi dla nich całkowicie naturalne środowisko, do którego nie muszą się adaptować, bo postrzegają je jako „ojczyste". Po raz pierwszy tego terminu użył w swoim rozdziale w 2001 roku Marc Prensky, opisując pokolenie osób, które urodziły się w czasach, gdy technologie informatyczne dynamicznie się upowszechniały i zaczęły wkraczać w codzienne życie zwykłego człowieka. Internet przestawał powoli być domeną elit i pojawiał się w licznych gospodarstwach domowych, przeobrażając dotychczasową rzeczywistość i zapraszając do tej nowej – wirtualnej (Jabłońska, 2018).

Dzisiaj dzieci i nastolatki nie znają świata bez komputera, a Internet istniał dla nich „od zawsze", bowiem już kilkumiesięczne dzieci dostają do ręki smartfona i szybko uczą się go obsługiwać. Internet oferuje młodym ludziom niemal nieograniczone możliwości rozwoju, ale równocześnie naraża ich na szereg zagrożeń związanych z kontaktem z niepożądanymi treściami

czy cyberprzemocą. Aktualnie dla dzieci Internet pełni funkcję socjalizacyjną, edukacyjną i kulturową, ułatwia samokształcenie, rozwój zainteresowań oraz nabywanie kompetencji cyfrowych, które stanowią niezbędny element funkcjonowania w społeczeństwie wiedzy, oraz pozwala na stały kontakt z rówieśnikami. Jednocześnie należy zauważyć, że cyberprzestrzeń jest środowiskiem ambiwalentnym – sprzyja rozwojowi, ale także rodzi liczne zagrożenia. Nadmierna ekspozycja na bodźce cyfrowe może prowadzić do rozproszenia uwagi, spłycenia procesów poznawczych oraz obniżenia zdolności koncentracji. Istnieje również ryzyko uzależnienia od Internetu, które – jak wskazują badania – może skutkować izolacją społeczną, obniżeniem nastroju, a nawet zaburzeniami emocjonalnymi. Cyberprzemoc, hejt czy kontakt z nieodpowiednimi treściami stanowi kolejne czynniki negatywnie oddziałujące na rozwój psychospołeczny młodych użytkowników.

Pedagodzy zwracają uwagę, że proces kształtowania tożsamości w epoce cyfrowej nabiera nowych wymiarów. Media społecznościowe stały się przestrzenią autoprezentacji i poszukiwania akceptacji, więc młodzież często konstruuje w sieci alternatywne obrazy własnego ja, które nie zawsze są zgodne z rzeczywistością offline, ale pozytywny odbiór i wirtualna aprobata dają rzeczywiste emocjonalne zaspokojenie potrzeb (Solecki, 2017). „Ten „realny świat cyfrowy" jest praktycznie zsynchronizowany z ich dobrostanem społecznym, psychicznym, somatycznym i nie jest to oddziaływanie marginalne, niszowe, ale nabrało cech zjawiska pokoleniowego" (NASK, 2023). Z perspektywy wychowawczej oznacza to konieczność wspierania dzieci w rozwijaniu kompetencji cyfrowych, medialnych i emocjonalnych.

Współczesne zagrożenia w cyberprzestrzeni

Rozwój Internetu i technologii mobilnych wprowadził dzieci i młodzież w przestrzeń, w której tradycyjne formy relacji społecznych, nauki i rozrywki uległy znaczącym przemianom. Dla najmłodszych użytkowników, charakteryzujących się ograniczoną dojrzałością emocjonalną i poznawczą, zagrożenia te mogą przybrać szczególnie dotkliwe formy. W literaturze naukowej oraz w raportach instytucji publicznych wskazuje się na kilka najczęściej występujących zjawisk: cyberprzemoc, grooming, sexting, uzależnienie od Internetu, dezinformację oraz nadużycia danych osobowych.

Cyberbullying, czyli tzw. cyberprzemoc, to forma agresji realizowanej przy użyciu technologii informacyjno-komunikacyjnych. Cyberbullying definiowany jest najczęściej jako ciąg aktów agresji. Są one w sposób celowy i powtarzalny kierowane przeciwko innej osobie, która nie może się obronić, doświadcza bowiem bezradności w tym zakresie, co wynika z charakteru tych aktów agresji, które są: anonimowe, niewidoczne, asynchroniczne i tekstualne. Otóż brak bezpośredniego kontaktu sprawcy z jego ofiarą uniemożliwia wystąpienie mechanizmów hamujących agresję i poczucie empatii wobec osoby krzywdzonej (Fundacja Orange, 2019). Pojęcie cyberbullyingu powstało na podstawie terminu „*bullying"*, który w literaturze był wykorzystywany przez badaczy najczęściej do wyjaśniania zjawiska agresji rówieśniczej w szkole i poza nią. Bullying charakteryzuje się triadą cech: intencjonalnością, powtarzalnością i nierównością sił. Wykorzystanie do agresji rówieśniczej technologii komunikacyjnych przyniosło nowy typ bullyingu – cyberbullying, który obejmuje działania takie jak: wyzywanie, ośmieszanie, upokarzanie, rozpowszechnianie kompromitujących zdjęć lub filmów, podszywanie się pod kogoś, a także wykluczanie z grup internetowych (Pyżalski, 2012)

Według raportu *Nastolatki 3.0* przygotowanego przez NASK, aż 29,7% polskich uczniów doświadczyło wyzywania w sieci, 22,8% było obiektem ośmieszania, a 10,5% – szantażu lub gróźb w środowisku internetowym. Zjawisko to wywołuje poważne skutki psychologiczne: obniżenie samooceny, poczucie wstydu, izolację, a w skrajnych przypadkach – zaburzenia depresyjne i próby samobójcze (NASK, 2023).

Cyberprzemoc jest szczególnie niebezpieczna, gdyż jej oddziaływanie jest potencjalnie nieograniczone – materiał opublikowany w Internecie może być wielokrotnie udostępniany i niełatwo go usunąć. Jak zauważa prof. Jacek Pyżalski: Internet sprzyja wzmacnianiu agresji poprzez anonimowość i brak bezpośredniego kontaktu z ofiarą, co obniża empatię sprawcy (Pyżalski, 2012).

Innym zagrożeniem dla młodych użytkowników Internetu jest g*rooming*, czyli proces nawiązywania relacji przez osobę dorosłą z dzieckiem w celu jego wykorzystania seksualnego lub emocjonalnego. Sprawca stosuje manipulację, wzbudza zaufanie, wykorzystuje potrzebę akceptacji, a następnie doprowadza do uzyskania intymnych treści lub spotkania w świecie rzeczywistym. Zjawisko to stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa dzieci w sieci. W raporcie EUROPOL zwrócono uwagę,

że pandemia COVID-19 doprowadziła do nasilenia aktywności sprawców przestępstw na tle seksualnym w Internecie. Grooming często odbywa się poprzez komunikatory, gry online lub media społecznościowe, a dzieci – ze względu na brak świadomości zagrożeń – rzadko informują o takich kontaktach dorosłych (Europol, 2022).

W Polsce art. 200a § 2 Kodeksu karnego penalizuje nawiązywanie kontaktu z małoletnim w celu jego wykorzystania seksualnego (Kodeks karny, 1997; Fundacja Instytut Cyberbezpieczeństwa, 2023). Jednak praktyka pokazuje, że wykrywalność takich czynów jest niska, co wynika z trudności w identyfikacji sprawców działających anonimowo.

Sexting, definiowany jako przesyłanie lub publikowanie własnych treści erotycznych – zdjęć, filmów lub wiadomości – jest coraz częściej obserwowanym zjawiskiem wśród młodzieży. Dla wielu nastolatków stanowi on formę flirtu lub wyraz zaufania, jednak konsekwencje mogą być dramatyczne, bowiem udostępnione materiały mogą zostać upublicznione bez zgody ich autora, co prowadzi do upokorzenia, szantażu, a w konsekwencji nawet prób samobójczych. Według raportu *EU Kids Online Polska 2018*, ok. 11% młodych użytkowników Internetu przyznało, że wysyłało lub otrzymywało zdjęcia o charakterze intymnym (Fundacja Orange, 2019). Natomiast niespełna tylko 2% rodziców zadeklarowało, iż wie o tego typu aktywności swojego dziecka w sieci (NASK, 2023). Sexting wśród nieletnich bywa też traktowany jako przestępstwo – zgodnie z art. 202 § 3 Kodeksu karnego zakazane jest posiadanie lub rozpowszechnianie treści pornograficznych z udziałem małoletnich (Kodeks karny, 1997). Tym samym, działania podejmowane przez młodzież w sposób nieświadomy mogą skutkować odpowiedzialnością karną. Jak podkreśla prof. Jadwiga Izdebska: „wczesna edukacja seksualna i cyfrowa powinna kształtować świadomość granic prywatności, odpowiedzialności i wzajemnego szacunku w relacjach online" (Izdebska, 2020).

Nadmierne korzystanie z Internetu i gier sieciowych prowadzi do tzw. uzależnienia behawioralnego. Światowa Organizacja Zdrowia (WHO) w 2019 r. uznała *gaming disorder* za jednostkę chorobową, charakteryzującą się utratą kontroli nad czasem spędzanym w grze, zaniedbywaniem obowiązków i pogorszeniem relacji społecznych (WHO, 2019).

Badania polskich uczniów wskazują, że ponad 10% młodych osób przejawia symptomy uzależnienia od Internetu. Skutkami są problemy

z koncentracją, zaburzenia snu, izolacja społeczna, a także obniżenie wyników w nauce. W opinii Anny Andrzejewskiej uzależnienie od mediów cyfrowych jest współczesną formą ucieczki od rzeczywistości, w której młody człowiek poszukuje kompensacji emocjonalnej i poczucia kompetencji (Andrzejewska, 2014). Profilaktyka wymaga zatem nie tylko ograniczania czasu przed ekranem, lecz także rozwijania umiejętności społecznych i wsparcia psychologicznego dzieci i młodzieży. Wraz z rozwojem mediów społecznościowych pojawiło się zjawisko tzw. *infodemii* – nadmiaru niezweryfikowanych informacji. Dzieci i młodzież, pozbawione umiejętności krytycznego myślenia medialnego, stają się łatwym celem manipulacji i dezinformacji.

Według badań EU Kids Online, aż 46% polskich nastolatków miało kontakt z treściami zawierającymi przemoc, a 29% – z mową nienawiści (Fundacja Orange, 2019). Wzmacnia to postawy agresywne, prowadzi do desensytyzacji, czyli znieczulenia emocjonalnego i sprzyja polaryzacji społecznej. Ponadto młodzież narażona jest na kontakt z treściami promującymi autodestrukcję, zaburzenia odżywiania, samookaleczanie czy ekstremizm. Jak zauważa prof. Maciej Tanaś: media elektroniczne kreują świat bez wartości granicznych, w którym młody człowiek bez właściwego przygotowania nie jest w stanie odróżnić dobro od zła (Tanaś, 2024).

Dzieci i młodzież są szczególnie narażone na manipulacje socjotechniczne – podszywanie się pod znajomych, wyłudzanie danych, haseł, a nawet pieniędzy. Brak doświadczenia i ufność wobec innych użytkowników sprawiają, że młodzi internauci stają się łatwym celem cyberprzestępców.

Z raportu CERT Polska wynika, że liczba prób phishingu i kradzieży danych osobowych rośnie z roku na rok, a część ataków kierowana jest bezpośrednio do młodzieży w grach online i mediach społecznościowych (CERT Polska, 2024). Zagrożenia te mają nie tylko wymiar finansowy, lecz także psychologiczny – utrata kontroli nad danymi prowadzi do lęku, poczucia wstydu i utraty zaufania do otoczenia. Dlatego edukacja w zakresie bezpiecznego korzystania z sieci, ochrony haseł i danych osobowych powinna stanowić kluczowy element programów profilaktycznych.

Aspekty prawne i instytucjonalne ochrony dzieci w sieci

Rozwój usług cyfrowych oraz rosnąca aktywność dzieci i młodzieży w Internecie powodują, że tradycyjne instrumenty ochrony prawnej wymagają

adaptacji. Pojawiają się szczególne zagrożenia: kontakty z predatoryjnymi sprawcami, rozpowszechnianie materiałów seksualnych z udziałem nieletnich, cyberbullying, manipulowanie, targetowanie reklamowe oraz naruszenia prywatności. Prawo musi równocześnie chronić dzieci i respektować ich prawa, np. prawo do wyrażania poglądów, co stawia wyzwania wykładni i stosowania norm. Konwencja o prawach dziecka ustanawia ramę wartościową, natomiast państwa mają obowiązek zapewnić ochronę i środki zapobiegawcze wobec zagrożeń dla dzieci (Konwencja o prawach dziecka, 1989).

Polski Kodeks karny przewiduje szereg przestępstw, które w praktyce obejmują także zachowania w cyberprzestrzeni związane z krzywdzeniem małoletnich. Wśród kluczowych typów znajdują się: seksualne wykorzystanie małoletniego (art. 200), elektroniczna korupcja seksualna małoletniego (art. 200a), propagowanie pedofilii (art. 200b), jak również ogólne typy przestępstw, takie jak groźby, znieważenie czy stalking, gdy są popełniane wobec nieletnich za pomocą środków komunikacji elektronicznej. W praktyce ściganie tych czynów wymaga współpracy służb ścigania z operatorami platform oraz specjalistycznych procedur dowodowych.

W Polsce obowiązują też akty regulujące działalność usług internetowych i ochronę danych osobowych: ustawa o świadczeniu usług drogą elektroniczną reguluje obowiązki usługodawców, w tym zasady obsługi zgłoszeń dotyczących nielegalnych treści oraz kwestie odpowiedzialności usługodawców (Ustawa o świadczeniu usług drogą elektroniczną, 2002).

Ponadto istnieje ustawa o ochronie danych osobowych (UODO) (wdrożenie RODO/GDPR do porządku krajowego) oraz akty wykonawcze i wytyczne Prezesa UODO, które dotyczą przetwarzania danych dzieci (np. publikowanie zdjęć dzieci, profilowanie reklamowe skierowane do małoletnich) (Ustawa o ochronie danych osobowych, 2018).

Rozporządzenie Unii Europejskiej 2016/679 (RODO/GDPR) zawiera szczególne uregulowania dotyczące dzieci, przede wszystkim art. 8 – warunki zgody w odniesieniu do usług społeczeństwa informacyjnego: przetwarzanie danych osobowych dziecka jest zgodne z prawem, gdy dziecko ma co najmniej 16 lat; państwa członkowskie mogą obniżyć ten próg do nie mniej niż 13 lat (Unia Europejska, 2016). W praktyce Polska zachowała próg 16 lat, to znaczy, że osoba poniżej 16 lat wymaga zgody przedstawiciela ustawowego przy korzystaniu z usług on-line wymagających zgody. Przepisy

RODO wprowadzają też zasady szczególnej ochrony dzieci. Problematyczne jednak w praktyce są mechanizmy weryfikacji wieku i potwierdzania zgody rodzica.

Unia Europejska regulowała też obszar przeciwdziałania seksualnemu wykorzystywaniu dzieci – np. dyrektywa 2011/93/UE w sprawie zwalczania nadużyć seksualnych i pornografii dziecięcej, instrumenty te wymagają od państw członkowskich penalizacji określonych zachowań oraz współpracy transgranicznej (w tym z Europolem) (Dyrektywa 2011/93/UE, 2011). W praktyce dyrektywa kształtuje krajowe kody karne i współpracę międzynarodową w ściganiu przestępstw seksualnych wobec dzieci.

Konwencja z 1989 r. (UNCRC) ustanawia ramę praw dziecka, z obowiązkiem państw stron do zapewnienia odpowiedniej ochrony, edukacji i środków zapobiegawczych. W kontekście cyfrowym Komitet Praw Dziecka oraz wytyczne ONZ podkreślają obowiązek państw do aktualizacji prawa w celu ochrony dzieci przed zagrożeniami w sieci, przy jednoczesnym poszanowaniu ich praw do informacji i wyrażania poglądów (Komitet Praw Dziecka ONZ, 2021).

W polskim porządku prawnym przestępstwa przeciwko wolności seksualnej i obyczajności oraz przestępstwa związane z rozpowszechnianiem treści pornograficznych z udziałem nieletnich stanowią szczególnie surowo penalizowane kategorie (art. 197-201 k.k., w tym art. 200, 200a, 200b). Przestępstwa te obejmują czyny dokonywane online, takie jak: grooming, elektroniczne nakłanianie do czynności seksualnych, produkcja i udostępnianie materiałów. Ponadto przestępstwa powszechne (np. stalking, groźby, zniesławienie) mogą przybrać formę cyberprzestępstw, gdy są popełniane w sieci wobec małoletnich (Kodeks karny, 1997).

Skuteczne ściganie wymaga umiejętnego gromadzenia dowodów elektronicznych, międzynarodowej współpracy oraz współdziałania z platformami cyfrowymi w zakresie dostępu do danych i treści. DSA oraz instrumenty UE mają ułatwić współpracę i wymianę informacji, ale w praktyce bariery proceduralne utrudniają działania (Unia Europejska, 2022). Polskie przepisy przewidują sankcje karne, takie jak: kara pozbawienia wolności, grzywna, zakazy działalności za czyny przeciwko małoletnim. W orzecznictwie i praktyce karnej coraz częściej pojawiają się środki prewencyjne i zabezpieczające, czyli nadzór, zakazy kontaktu z dziećmi, ale istnieje potrzeba

lepszej specjalizacji organów ścigania i sądownictwa w sprawach cyberprzestępczości wobec dzieci.

Ochrona dzieci w cyberprzestrzeni wymaga kompleksowego podejścia łączącego normy karne, ochronę danych, regulacje sektorowe oraz instrumenty międzynarodowe. RODO i DSA stworzyły istotne narzędzia prawne, lecz istnieją realne luki – techniczne, proceduralne i międzynarodowe – które utrudniają pełne zabezpieczenie małoletnich. Konieczne są zarówno techniczne innowacje zgodne z prawami człowieka, jak i polityczne decyzje wzmacniające współpracę międzynarodową i egzekucję odpowiedzialności platform.

Podsumowanie

Cyberbezpieczeństwo dzieci i młodzieży stanowi jedno z najważniejszych wyzwań współczesnego społeczeństwa informacyjnego. Rozdział ukazuje, że rozwój technologii cyfrowych, choć niesie ogromne możliwości edukacyjne i komunikacyjne, jednocześnie stwarza liczne zagrożenia dla najmłodszych użytkowników Internetu. Zjawiska takie jak cyberprzemoc, sexting, grooming, uzależnienie od mediów cyfrowych, dezinformacja czy manipulacje danymi osobowymi stają się coraz bardziej powszechne, wpływając negatywnie na rozwój emocjonalny, społeczny i moralny młodego pokolenia.

Autorzy podkreślają, że skuteczna ochrona dzieci i młodzieży w przestrzeni cyfrowej wymaga zintegrowanego i wielowymiarowego podejścia, łączącego aspekty edukacyjne, prawne, psychologiczne i technologiczne. Niezbędne jest systemowe włączenie edukacji cyfrowej do programów nauczania oraz rozwijanie kompetencji medialnych, krytycznego myślenia i świadomości zagrożeń zarówno wśród uczniów, jak i dorosłych rodziców oraz nauczycieli. Współpraca pomiędzy szkołą, rodziną, instytucjami publicznymi i organizacjami społecznymi stanowi warunek skutecznego przeciwdziałania cyberzagrożeniom.

Z perspektywy prawnej konieczne jest dalsze doskonalenie przepisów krajowych i unijnych oraz usprawnienie mechanizmów egzekwowania prawa w zakresie ochrony małoletnich użytkowników sieci. Jednocześnie podkreśla się znaczenie działań profilaktycznych, kampanii informacyjnych i wsparcia psychologicznego dla dzieci dotkniętych cyberprzemocą lub innymi formami nadużycia.

Podsumowując, bezpieczeństwo cyfrowe dzieci i młodzieży nie może opierać się wyłącznie na technicznych narzędziach ochronnych, lecz wymaga kształtowania dojrzałych postaw, empatii i odpowiedzialności w korzystaniu z technologii. Tylko poprzez kompleksowe i długofalowe działania możliwe jest stworzenie środowiska cyfrowego, które sprzyja rozwojowi młodego człowieka, a jednocześnie skutecznie chroni go przed zagrożeniami współczesnego świata.

Literatura

1. Andrzejewska, A. (2014). *Dzieci i młodzież w sieci zagrożeń realnych i wirtualnych: aspekty teoretyczne i empiryczne*. Difin.
2. CERT Polska. (2024*). Raport roczny z działalności CERT Polska w 2023 roku.* CERT Polska.
3. *Dyrektywa Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej oraz zastępująca decyzję ramową Rady 2004/68/WSiSW*. (2011). Dz.Urz. UE L 335 z 17.12.2011.
4. Europol. (2022). *Internet Organised Crime Threat Assessment 2022* (IOCTA). Europol.
5. Fundacja Instytut Cyberbezpieczeństwa. (2023). *Problematyka tzw. „child grooming" – okiem prawnika*. Fundacja Instytut Cyberbezpieczeństwa.
6. Fundacja Orange. (2019). *Polskie badanie EU Kids Online 2018*. Fundacja Orange.
7. Izdebska, J. (2020). *Dziecko w świecie mediów elektronicznych: Teoria, badania, edukacja medialna*. Wydawnictwo Trans Humana.
8. Jabłońska, M. R. (2018). *Człowiek w cyberprzestrzeni: Wprowadzenie do psychologii Internetu.* Wydawnictwo Uniwersytetu Łódzkiego.
9. Komitet Praw Dziecka ONZ. (2021*). Komentarz ogólny nr 25 (2021) w sprawie praw dziecka w środowisku cyfrowym.*
10. Konieczniak, M. (2011). Poszukiwanie tożsamości w cyberprzestrzeni: Implikacje pedagogiczne. *Edukacja i Dialog, 5/6*, 8-19.
11. Konwencja o prawach dziecka. (1989). *Konwencja o prawach dziecka przyjęta przez Zgromadzenie Ogólne ONZ dnia 20 listopada 1989 r.* (Dz. U. z 1991 r. Nr 120, poz. 526).

12. Lévy, P. (2002). Drugi potop. W: M. Hopfinger (red.), *Nowe media w komunikacji społecznej w XX wieku*: *Antologia* (s. 373-390). Oficyna Naukowa.
13. NASK. (2023). *Nastolatki 3.0: Raport z ogólnopolskiego badania uczniów i rodzic*ów. NASK – Państwowy Instytut Badawczy.
14. Pyżalski, J. (2012). *Agresja elektroniczna i cyberbullying jako nowe ryzykowne zachowania młodzieży.* Oficyna Wydawnicza „Impuls".
15. Unia Europejska. (2016). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych oraz w sprawie swobodnego przepływu takich danych* (Dz. Urz. UE L 119 z 4.05.2016).
16. Unia Europejska. (2022). *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych).* Dz.Urz. UE L 277 z 27.10.2022, s. 1-102.
17. Solecki, R. (2017). *Aktywność młodzieży w cyberprzestrzeni: Profilaktyka patologicznego używania Internetu*. Oficyna Wydawnicza Von Velke.
18. Tanaś, M. (red.). (2024). *Pedagogika, środki informatyczne i media*. Oficyna Wydawnicza Impuls.
19. Ustawa o ochronie danych osobowych. (2018). *Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych* (Dz. U. z 2018 r. poz. 1000).
20. Ustawa o świadczeniu usług drogą elektroniczną. (2002). *Ustawa z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną* (Dz. U. z 2002 r. Nr 144, poz. 1204 z późn. zm.).
21. *Ustawa z dnia 6 czerwca 1997 r.* – Kodeks karny (Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.).
22. WHO. (2019). *International Classification of Diseases, 11th Revision (ICD-11).* World Health Organization.
23. Wochnowicz, A. (2023). Cyberprzestrzeń w systemie militarnym bezpieczeństwa państwa. *Cybersecurity and Law, 2*(10), 51-69.