Zeszyty Naukowe
Zbliżenia Cywilizacyjne XIII (3)/2017

ISSN: 1896-4087
DOI: http://dx.doi.org/10.21784/ZC.2017.017

MATEUSZ OLCHANOWSKI
Uniwersytet w Białymstoku
Izba Adwokacka w Białymstoku

Bezpieczeństwo dzieci i młodzieży w cyberprzestrzeni na podstawie Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022

Safety of children and youth in cyberspace under the National Framework of Cyber Security Policy of the Republic of Poland for years 2017–2022

Streszczenie:
W pierwszej części artykułu przybliżony został problem odpowiedniego zabezpieczenia dzieci i młodzieży od zagrożeń występujących w cyberprzestrzeni. W dalszej kolejności autor pracy przybliżył regulacje „Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022" i zarazem dokonał ich analizy pod kątem zabezpieczenia w cyberprzestrzeni interesu najmłodszych. Intencją autora było m. in. zweryfikowanie czy zapewnienie bezpieczeństwa dzieci i młodzieży w cyberświecie jest dla rządu polskiego priorytetem, czy może jednak problem ten jest zupełnie ignorowany? Analiza poprzedzona jest przedstawieniem status quo polskich regulacji prawnych stojących na straży bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni. W podsumowaniu zawarte są wnioski, jakie autor wyciągnął z przedmiotowej analizy.
Słowa kluczowe: cyberbezpieczeństwo, cyberprzestrzeń

Abstract:
The first part of the article depicts the problem of adequate protection of children and young people against the dangers occurring in cyberspace. Subsequently, the

author of the paper described the 'National Framework of Cyber Security Policy of the Republic of Poland for years 2017–2022' and at the same time analysed it in terms of securing in cyberspace the interests of the youngest. The intention of the author was, among other things, to verify whether ensuring the safety of children and young people in cyberspace is a priority for the Polish Government or whether this problem is completely ignored. The analysis is preceded by the presentation of the status quo of Polish legal regulations that protect the safety of children and young people in cyberspace. The final part contains the conclusions the author drew from the analysis of the issue.
Keywords: cyber security; cyberspace

Wstęp

Postępujący rozwój technologiczny bezpośrednio rzutuje na życie każdego z nas. Znaczna część naszej aktywności zarówno społecznej jak i gospodarczej odbywa się w cyberprzestrzeni[1] lub przy jej użyciu. Jak trafnie zauważył M. Castells gdy tylko nowe technologie rozprzestrzeniły się, nastąpiło nasilenie się różnego rodzaju zachowań i użytków[2]. Jednak dynamiczny rozwój technologii informatycznych[3] przyczynia się nie tylko pozytywnych zmian w sferach życia jednostki, ale również do przekształcenia lub nasilenia obecnych oraz powstania nowych zagrożeń, często również o charakterze kryminalnym. Zachowanie bezpieczeństwa państwa i obywateli coraz częściej opiera się o kwestię cyberbezpieczeństwa[4]. Zgodnie ze stanowiskiem Najwyższej Izby Kontroli[5] bezpieczeństwo w cyberprzestrzeni nie jest w Pol-

[1] Zgodnie z definicją zawartą w Krajowych Ramach Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022, cyberprzestrzeń to przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami.

[2] M. Castells, *Społeczeństwo sieci*, Warszawa 2007, s. 23–24.

[3] T. R. Aleksandrowicz, *Świat w sieci. Państwa, społeczeństwa, ludzie w poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego*, Warszawa 2014, s. 62.

[4] M. Karnowska-Werner, *Zagrożenia bezpieczeństwa w cyberprzestrzeni,* [w:] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Warszawa 2014, s. 285.

[5] Informacja o wynikach kontroli NIK w sprawie realizacji przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP, KPB-4101-002-00/2014.

sce należycie chronione. Podkreślenia wymaga fakt, iż jednymi z głównych użytkowników Internetu są właśnie dzieci. Badania przeprowadzone w 2015 r. przez Centrum Badania Opinii Społecznej[6] wykazały, że 86% polskich dzieci i młodzieży w wieku od 6 do 19 lat korzysta z Internetu. Tendencja od lat jest stale rosnąca. Inne badania przeprowadzone przez Instytut NASK[7] wskazują, że ponad 90% nastolatków do 12 roku życia miało przynajmniej raz styczność z Internetem. Dla porównania odsetek dorosłych internautów w grupie wiekowej 45–54, wyniósł w analogicznym okresie 60%[8]. Wydawać się może, iż z wiekiem zainteresowanie jednostek cyberprzestrzenią spada. Paradoksalnie jednak to właśnie dorośli tworzą ramy prawne, mające na celu między innymi ochronę najmłodszych przed zagrożeniami płynącymi z cyberprzestrzeni. Takie zjawisko można nazwać swego rodzaju zbliżeniem cywilizacyjnym, gdzie nowoczesna i dynamicznie rozwijająca się technologia, użytkowana w przeważającej większości przez ludzi młodych spotyka się ze starym porządkiem prawnym, często nieprzygotowanym na problemy i zagrożenia zmieniającego się świata.

Dzieci i młodzież, ze względu na swój wiek i rozwój psychofizyczny, zasługują na szczególną ochronę prawną przed zagrożeniami Internetu. Zauważyć należy, że w sferze tej prym wiodą regulacje międzynarodowe wyznaczające standardy pojedynczym państwom[9]. Jednak to na władzach konkretnych państw, w tym Polski, leży obowiązek nie tylko prawny wynikający z przyjętych zobowiązań o charakterze międzynarodowym, ale i moralny zapewnienia nowemu pokoleniu bezpieczeństwa w cyberprzestrzeni.

[6] Centrum Badania Opinii Społecznej, Komunikat z badań nr 110/2015, http://www.cbos.pl [dostęp: 6.09.2017].

[7] Raport z badania Nastolatki 3.0, NASK, tabela 3a1.

[8] Centrum Badania Opinii Społecznej, Komunikat z badań nr 90/2015, http://www.cbos.pl [dostęp: 6.09.2017].

[9] Obok Konwencji Rady Europy o cyberprzestępczości z dnia 23 listopada 2001 r. (Dz. U. z 2015 r., poz. 728), wspomnieć należy również o Konwencji Rady Europy o ochronie dzieci przed seksualnym wykorzystaniem i niegodziwym traktowaniem w celach seksualnych sporządzonej w dniu 25 października 2007 r. w Lanzarote.

Cyberświat, który z biegiem czasu staje się coraz częściej światem alternatywnym, toczącym się równolegle do życia realnego, zasługuje na większą niż kiedykolwiek wcześniej uwagę. Prace nad tą kwestią powzięło Ministerstwo Cyfryzacji[10] tworząc Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022 (dalej: krajowe ramy lub dokument). Artykuł zawiera analizę wskazanego powyżej dokumentu w kontekście przytoczonych na wstępie uwag i zauważonych problemów. Autor będzie szukał odpowiedzi między innymi na pytanie: Czy zapewnienie bezpieczeństwa dzieci i młodzieży w cyberświecie jest dla rządu polskiego priorytetem, czy może jednak problem ten został pominięty? Rozważania te poprzedzi treściwe przedstawienie aktualnego stanu prawnego mającego na celu zagwarantowanie bezpieczeństwa dzieci i młodzieży w cyberświecie. Na końcu pracy zawarte są wnioski podsumowujące.

Bezpieczeństwo dzieci i młodzieży na gruncie aktualnego stanu prawnego w Polsce

Przed analizą i omówieniem zapisów znajdujących się w Krajowych Ramach Polityki Cyberbezpieczeństwa, należy zwięźle przybliżyć obecne regulacje prawne stojące na straży bezpieczeństwa dzieci i młodzieży w Internecie, gdyż to one są podstawowymi gwarancjami ochrony interesu najmłodszych. Najważniejszym aktem prawnym zapewniającym ochronę praw dzieci i młodzieży jest Konstytucja Rzeczypospolitej Polskiej[11]. W art. 72 ust. 1 nakłada ona na organy władzy publicznej obowiązek ochrony praw dziecka. Zgodnie z jego treścią, każdy ma prawo do żądania od organów państwowych ochrony

[10] Wraz z przedstawicielami Ministerstwa Obrony Narodowej, Ministerstwa Spraw Wewnętrznych i Administracji, Agencji Bezpieczeństwa Wewnętrznego, Rządowego Centrum Bezpieczeństwa i Biura Bezpieczeństwa Narodowego.

[11] Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r., nr 78 poz. 483 ze zm.

dziecka przed przemocą, okrucieństwem, wyzyskiem i demoralizacją[12].

W dalszej kolejności wskazać należy przepisy ustawy z dnia 6 czerwca 1997 r. – Kodeks karny[13], jako rozwinięcie gwarancji ustanowionych przez Konstytucję. Ustawa ta penalizuje szereg czynów społecznie szkodliwych, przez co spełnia nie tylko rolę ochronną wobec dzieci i młodzieży, ale również funkcję prewencyjną. Przepisy kodeksu odnoszą się wprost do cyberbezpieczeństwa dzieci i młodzieży penalizując zachowania będące cyberprzestępstwami, a więc czyny bezpośrednio popełnione w cyberprzestrzeni lub przy jej użyciu. Przede wszystkim są to zachowania o charakterze pedofilskim. Począwszy od elektronicznej korupcji seksualnej małoletniego (art. 200a § 1), a kończąc na czynach związanych z treściami pornograficznymi z udziałem małoletnich (art. 200b, art. 202). Biorąc pod uwagę szerokie ujęcie pojęcia „cyberprzestępczości" jako przestępczości mającej miejsce w cyberprzestrzeni[14], katalog czynów zabronionych jest obszerny. Ustawa obok czynów zabronionych pod groźbą kary określa szereg środków karnych. Ich celem jest ochrona dzieci i młodzieży przed osobami w stosunku, do których zachodzi obawa, iż mogłyby dopuścić się względem najmłodszych czynów kryminalnych[15].

Kolejnym ważnym aktem prawnym jest ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego[16] (dalej: k.p.k.). Przepisy tej ustawy umożliwiają skuteczne urzeczywistnianie norm prawa karnego materialnego. Regulacja prawna odnosi się między innymi do ważnej kwestii dowodów (w tym do dowodów cyfrowych[17]) i ich

[12] M. Gruchoła, *Ochrona użytkowników Internetu w państwach Unii Europejskiej,* Lublin 2012, s. 104.

[13] Dz. U. z 2016 r., poz. 189 ze zm.

[14] J. Kosiński, *Paradygmaty Cyberprzestępczości*, Warszawa 2015, s. 88.

[15] A. Ziółkowska, *Komentarz do art. 41 kodeksu karnego*, [w:] V. Konarska-Wrzosek, *Kodeks Karny. Komentarz*, Warszawa 2016, s. 247 i n.

[16] Dz. U. z 2015 r., poz. 1334 ze zm.

[17] Inna nazwa to „dowody elektroniczne".

zabezpieczenia w toku postępowań karnych[18]. Kodeks zawiera również szereg przepisów mających na celu zredukowanie do minimum negatywnych konsekwencji psychicznych najmłodszych wynikających z toczącego się postępowania karnego. W stosunku do osób małoletnich[19] obowiązują odmienne regulacje dotyczące ich przesłuchania (art. 185a k.p.k. oraz art. 185b k.p.k.).

Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022

W drodze uchwały nr 52/2017 z dnia 27 kwietnia 2017 r. Rada Ministrów przyjęła Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022[20]. W podtytule dokumentu widnieją słowa: poszanowanie praw i wolności w cyberprzestrzeni. Jak się wydaje, sygnalizuje to, iż dokument będzie dotyczył uprawnień i swobód wszystkich podmiotów prawa, w tym dzieci i młodzieży. Dokument podzielony został na wstęp, kontekst strategiczny, zakres krajowych ram, wizję oraz cele główne i szczegółowe. Na końcu zawarte są punkty dotyczące zarządzania i finansowania oraz wyjaśnienia pojęć użytych w krajowych ramach.

Na wstępie autorzy zauważają, iż rozwój społeczno-gospodarczy coraz częściej zależny jest od szybkiego dostępu do informacji oraz jej wykorzystania. Bezpieczeństwo cyberprzestrzeni, jako narzędzia służącego do operacji na dużych zasobach danych jest więc przesłanką do zachowania bezpieczeństwa obrotu gospodarczego, poczucia bezpieczeństwa obywateli, sprawności funkcjonowania instytucji sektora publicznego, przebiegu procesów produkcyjnych i usługowych, a w rezultacie do ogólnie pojmowane bezpieczeństwa narodowego.

[18] A. Mroczek, A. Sułkowska, *Zabezpieczanie dowodu elektronicznego*, [w:] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Warszawa 2014, s. 199.

[19] Małoletniego poniżej lat 15 lub, który ukończył ten wiek lecz przesłuchanie go w innych warunkach mogłoby oddziałać negatywnie na jego psychikę.

[20] Załącznik do uchwały nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r.

W dalszej kolejności autorzy przytaczają kontekst strategiczny dokumentu wskazując, że jest on kontynuacją działań podejmowanych w latach ubiegłych[21]. Twórcy zwrócili uwagę, że rozwój systemów teleinformatycznych niesie ze sobą ryzyko związane z rosnącą liczbą niebezpieczeństw w sieci, co rzutuje na konieczność podjęcia spójnych działań w skali całego państwa. Zdaniem pomysłodawców zaproponowane przez nich ramowe działania przyczynią się do zwiększenia efektów działania organów ścigania oraz wymiaru sprawiedliwości w lokalizowaniu i zwalczaniu niezgodnych z prawem zachowań.

Punkt odnoszący się do zakresu krajowych ram polityki cyberbezpieczeństwa przedstawia zwięźle zawartość analizowanego dokumentu. Obok celów z zakresu bezpieczeństwa teleinformatycznego, w dokumencie znajdują się kierunki podejścia do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa. Z perspektywy bezpieczeństwa dzieci i młodzieży w sieci ujednolicenie projektów edukacyjnych i szkoleniowych wydaje się być dobrym pomysłem. Najmłodsi, jako ci, którzy są najbardziej podatni na wpływy, muszą być dobrze poinformowani o zagrożeniach płynących z cyberprzestrzeni, tak by sami mogli je wykrywać i zawczasu ich unikać. Zdaniem twórców krajowe ramy w przyszłości mają w sposób pośredni wpływać na życie obywateli poprzez przyjęcie z inicjatywy Rady Ministrów przepisów prawa powszechnego. W ocenie autora jest to bardzo ważna zapowiedź zmian legislacyjnych w zakresie cyberbezpieczeństwa niezawierająca zarazem żadnych konkretów. Należy spodziewać się, że zmiany prawa, o których mowa dotykać będą bezpośrednio problemów i celów wskazanych w badanym dokumencie.

Wizją autorów dokumentu jest państwo polskie w 2020 r., bardziej odporne na zagrożenia płynące z cyberprzestrzeni. Celem głównym krajowych ram jest zapewnienie wysokiego poziomu bezpieczeństwa

[21] Mowa o przyjętej przez rząd w 2013 r. Polityce Ochrony Cyberprzestrzeni Rzeczypospolitej Polskiej. Więcej w: J. Skrzypczak, *Polityka ochrony cyberprzestrzeni RP,* „Przegląd Strategiczny" 2014, nr 7, s. 133 i n.

sektora publicznego i prywatnego oraz obywateli w zakresie korzystania z usług cyfrowych. Czterema celami szczegółowymi są: skoordynowanie działań w przeciwdziałaniu incydentom naruszającym bezpieczeństwo systemów teleinformatycznych istotnych dla funkcjonowania państwa, wzmacnianie zdolności do przeciwdziałania cyberzagrożeniom, zwiększanie potencjału narodowego oraz kompetencji w zakresie cyberbezpieczeństwa oraz zbudowanie w tożsamym zakresie silnej pozycji Polski na arenie międzynarodowej. Poszczególne cele są rozbudowane w dalszej części dokumentu. Z punktu widzenia bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni, najważniejszy jest pierwszy, drugi i trzeci z wymienionych celów szczegółowych.

Pierwszy z celów osiągnięty ma zostać poprzez zmiany legislacyjne w obszarze bezpieczeństwa w cyberprzestrzeni. Zamiarem autorów jest dokonanie przeglądu obecnych przepisów prawa w celu ich harmonizacji. Konkretnym prognostykiem dotyczącym zmian w ustawodawstwie jest zapowiedź implementacji Dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii[22]. Sama treść dyrektywy nie odnosi się bezpośrednio do bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni, jednak już w art. 1 zaznacza, iż jej implementacja musi przebiegać bez uszczerbku dla Dyrektywy Parlamentu Europejskiego i Rady 2011/93/UE z dnia 13 grudnia 2011 r. w sprawie zwalczania niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci oraz pornografii dziecięcej, zastępującej decyzję ramową Rady 2004/68/WSiSW[23]. Taki zapis poniekąd wyznacza priorytety Unii Europejskiej wskazując, iż ochrona najmłodszych przed zagrożeniami cyberświata jest priorytetem w budowie wspólnego bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej. Twórcy krajowych ram zauważyli problem dynamiki procesów zachodzących w cyberprzestrzeni i zasygnalizo-

[22] Dz. U. UE 2016 L194.
[23] Dz. U. UE L 335 z 17.12.2011, s. 1.

wali konieczność śledzenia zachodzących tam zmian tak, by w porę podjąć inicjatywę nowelizacji przepisów prawa.

Podwyższenie kompetencji ośrodków naukowych w zakresie bezpieczeństwa w cyberprzestrzeni, zarówno sprawne wykrywanie, jak i zwalczanie cyberzagrożeń przyczyni się korzystnie do ochrony najmłodszych użytkowników systemów informatycznych. Wzmocnienie potencjału w zakresie profilaktyki zagrożeń w cyberprzestrzeni odbywać się ma między innymi poprzez zbudowanie zdolności analitycznych w ocenie cyberzagrożeń oraz weryfikacji konkretnych incydentów. Zdaniem autora w dobie dynamicznego rozwoju nowoczesnych technologii, wczesna i dogłębna analiza zagrożeń przypisana Narodowemu Centrum Cyberbezpieczeństwa[24], jeśli zostanie odpowiednio spożytkowana, może przyczynić się do zwiększenia bezpieczeństwa najmłodszych. Wartym zauważyć, iż to właśnie ten podmiot zajmuje się obsługą zgłoszeń szkodliwych i nielegalnych treści, w tym treści pornograficznych z udziałem nieletnich[25].

Zwiększenie potencjału narodowego oraz umiejętności w zakresie bezpieczeństwa cyberprzestrzeni w kontekście ochrony praw i wolności nieletnich obywateli ma nastąpić poprzez, między innymi, edukację z zakresu cyberbezpieczeństwa. Twórcy dokumentu zakładają, że skuteczna edukacja zależy od jak najwcześniejszego rozpoczęcia procesu kształcenia, dlatego też zakładają, że nastąpi to już na etapie wczesnoszkolnym. Autorzy zakładają opracowanie i wdrożenie zmian programowych do podstaw nauczania w szkole. Ponadto zaplanowano stworzenie i rozpoczęcie kursów dla nauczycieli informatyki oraz zmiany w kształceniu podyplomowym nauczycieli, tak by podnieść ich kwalifikacje z zakresu bezpieczeństwa w cyberprzestrzeni. Propozycje przyjęte w krajowych ramach należy ocenić bardzo pozytywnie. Zarazem jednak autorzy nie dostrzegli, iż dzieci i młodzież korzystają już nie tylko z Internetu w celu komunikacji i rozrywki, ale

[24] Centrum działa w strukturze Naukowej i Akademickiej Sieci Komputerowej (NASK).

[25] Poprzez portal internetowy dyzurnet.pl.

również coraz częściej czerpią z niego wiedzę[26]. Należy zastanowić się, czy oprócz zmian w *stricte* tradycyjnych formach edukacji, nie opracować i wdrożyć systemu edukacji bezpośrednio w cyberprzestrzeni, czyli tam gdzie zagrożenia mają swoją genezę. Przykładowo poprzez aplikacje internetowe lub przy pomocy komunikatów w witrynach internetowych odwiedzanych głównie przez najmłodszych.

Realizacji celu przyświecać ma również uwrażliwianie obywateli (dzieci, młodzieży, rodziców) na cyberzagrożenia. Opracowane mają zostać kampanie celowane do różnych grup społecznych w zakresie edukacji o prawach i wolnościach w cyberświecie. Zadaniem administracji publicznej będzie również wspieranie operatorów i dostawców usług cyfrowych w zakresie podejmowania działań edukacyjnych. Końcowym celem ma być zapewnienie użytkownikom Internetu dostępu do wiedzy umożliwiającej zrozumienie zagrożeń w cyberprzestrzeni i wczesnego ich unikania. Zaproponowane rozwiązania, zdaniem Autora, przyczynią się korzystnie do prewencji wobec cyberzagrożeń. Ukierunkowane kampanie społeczne, przede wszystkim te skierowane do dzieci i młodzieży to dobry prognostyk na przyszłość. Nie od dziś wiadomo, iż lepiej jest zapobiegać niż leczyć zaniedbane problemy. Uświadamianie najmłodszych o zagrożeniach płynących z cyberprzestrzeni za pomocą przekazów sprofilowanych do ich grupy wiekowej, może zasadniczo zwiększyć ich skuteczność.

W końcowej części dokument zawiera regulacje dotyczące zarządzania krajowymi ramami. Koordynatorem przyjętych działań będzie minister właściwy do spraw informatyzacji. Po dwóch latach obowiązywania nastąpi pierwszy przegląd i kontrola efektów oddziaływania krajowych ram. W ciągu sześciu miesięcy ma zostać przygotowany plan działań na rzecz wdrożenia krajowych ram polityki cyberbezpieczeństwa. Na obecnym etapie finansowanie wdrażania krajowych ram ma odbywać się w ramach planów finansowych poszczególnych jednostek uczestniczących w przedsięwzięciu. Jednak docelowo finansowanie zagwarantowane ma zostać w Wieloletnim Programie doty-

[26] Raport z badania *Nastolatki 3.0*, NASK, s. 29.

czącym cyberbezpieczeństwa ujętym w ustawie budżetowej. Dokument zamyka słownik pojęć użytych w Krajowych Ramach Polityki Cyberbezpieczeństwa RP. Propozycje zagwarantowania środków przeznaczonych na ochronę bezpieczeństwa w cyberprzestrzeni już na etapie konstruowania ustawy budżetowej to właściwa droga. Praktycznie nieograniczona ilość podmiotów narażonych na cyberzagrożenia skutkuje koniecznością zaangażowania znacznej sumy pieniędzy na efektywną walkę z tym negatywnym zjawiskiem.

Podsumowanie

Na pytanie zawarte we wstępie nie da się udzielić odpowiedzi za pomocą znaków systemu binarnego (0,1). W ocenie autora, twórcy krajowych ram polityki cyberbezpieczeństwa dostrzegają konieczność ochrony bezpieczeństwa dzieci i młodzieży w cyberprzestrzeni, jednak nie można stwierdzić, iż jest to jeden z priorytetów przyjętego dokumentu. Analiza jego treści prowadzi do wniosku, iż kwestia ochrony praw dzieci i młodzieży jest w nim rzadko poruszana. Problem zapewnienia cyberbezpieczeństwa najmłodszych potraktowany został przez twórców po „macoszemu". Krajowe ramy bardziej koncentrują się na ochronie państwa, jako całości, niż na bezpieczeństwie konkretnych grup społecznych, w tym tych najbardziej bezbronnych. Z jednej strony zagadnienie zostało dostrzeżone przez autorów, z drugiej natomiast potraktowane *minorum gentium* – bez poświecenia mu należytej uwagi. Należy podkreślić, że poprzedzający dokument – przyjęta w 2013 r. Polityka Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, był znacznie bardziej rozbudowany w zakresie ochrony dzieci i młodzieży.

Autorzy Krajowych Ram skupili się głównie na przeciwdziałaniu cyberzagrożeniom poprzez edukację. Pomimo, iż dokument skupia się bardziej na nauczaniu najmłodszych niż na wprowadzeniu przepisów prawa gwarantujących ich bezpieczeństwo w cyberprzestrzeni, to w pracach nad krajowymi ramami nie uczestniczyli przedstawiciele

Ministerstwa Edukacji Narodowej. Naturalnie wydaje się, iż propozycje zmian w programach kształcenia winny przebiegać we współpracy właśnie z tym działem administracji rządowej. Skutkiem braku współpracy między Ministerstwem Edukacji Narodowej, Ministerstwem Cyfryzacji a organami ścigania jest to, że nie ma w Polsce opracowanych wytycznych dotyczących zapobiegania i przeciwdziałania cyberprzemocy wśród dzieci i młodzieży[27].

Propozycje dotyczące zmian w kształceniu najmłodszych wydają się niewystarczające. Działania prewencyjne, choć bardzo ważne, nie zastąpią organów wymiaru sprawiedliwości w sytuacji, gdy dojdzie już do naruszenia prawa. Zasygnalizowane w krajowych ramach propozycje zmian w prawie autor ocenia, jako zbyt powierzchowne. Polskie akty normatywne nie są do końca zgodne z postanowieniami multilateralnych umów międzynarodowych[28] dotyczących cyberbezpieczeństwa dzieci i młodzieży. Pomimo krytyki przez doktrynę, autorzy krajowych ram zdają się nie dostrzegać tego problemu. W dalszym ciągu istnieje potrzeba unifikacji polskiego porządku prawnego z regulacjami ponadpaństwowymi. Brak jest natomiast zapowiedzi o konkretnych działaniach mających na celu dostosowanie prawa polskiego do wymogów międzynarodowych. W ocenie autora, takie niedociągnięcie może wynikać z braku przedstawicieli Ministerstwa Sprawiedliwości przy pracach nad dokumentem. Pomijając powyższe mankamenty wskazać należy, że krajowe ramy stanowią dobry fundament do dalszych prac w tym zakresie[29].

Zaniedbania organów władzy wykonawczej powodują sytuację, w której cierpią najmłodsi. Cyberprzestępstwa na szkodę dzieci i mło-

[27] Informacja o wynikach kontroli Najwyższej Izby Kontroli w sprawie zapobiegania i przeciwdziałania przemocy wśród dzieci i młodzieży, LIK.410.002.00.2017.

[28] A. Adamski, *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, [w:] G. Szpor, *Internet. Ochrona wolności, własności i bezpieczeństwa*, Warszawa 2011, s. 348.

[29] A. Kozłowski, *Bezpieczna Polska w cyfrowej erze. Strategia Cyberbezpieczeństwa na lata 2017–2022 [ANALIZA],* http://www.cyberdefence24.pl/555852,bezpieczna-polska-w-cyfrowej-erze-strategia-cyberbezpieczenstwa-na-lata-2017-2022-analiza, [dostęp: 11.09.2017].

dzieży utrzymują się na wysokim poziomie, a niektóre z nich wykazują tendencję rosnącą[30]. Zgodnie z brzmieniem krajowych ram ich postanowienia mogą być na bieżąco aktualizowane. W tej kwestii należałoby wymagać od autorów dokumentu rewizji zapisów i ich dostosowania do potrzeb, po konsultacji z szerszym (niż pierwotne) gremium specjalistów z tego zakresu.

Kompleksowa spojrzenie na zaproponowane zmiany będzie możliwe dopiero po analizie następstw przyjętego dokumentu. Na pierwsze efekty funkcjonowania Krajowych Ram Polityki Cyberbezpieczeństwa RP należy jednak poczekać. Autorzy dopiero po dwóch latach przeprowadzą pierwszy planowany przegląd, dokonają oceny efektów oddziaływania przyjętego dokumentu, a następnie przedstawią je Radzie Ministrów[31].

Bibliografia:

Adamski A., *Konwencja Rady Europy o cyberprzestępczości i kwestia jej ratyfikacji przez Polskę*, [w:] G. Szpor, *Internet. Ochrona wolności, własności i bezpieczeństwa*, C.H. Beck, Warszawa 2011.

Aleksandrowicz T. R., *Świat w sieci. Państwa, społeczeństwa, ludzie w poszukiwaniu nowego paradygmatu bezpieczeństwa narodowego,* Difin, Warszawa 2014.

Castells M., *Społeczeństwo sieci*, PWN, Warszawa 2007.

Gruchoła M., *Ochrona użytkowników Internetu w państwach Unii Europejskiej,* Wydawnictwo KUL, Lublin 2012.

Karnowska-Werner M., *Zagrożenia bezpieczeństwa w cyberprzestrzeni*, [w:] M. Górka, *Cyberbezpieczeństwo jako podstawa bezpiecznego państwa i społeczeństwa w XXI wieku*, Difin, Warszawa 2014.

[30] Ministerstwo Sprawiedliwości, Skazania prawomocne – dorośli – wg rodzajów przestępstw i wymiaru kary w l.2008-2016, https://isws.ms.gov.pl/pl/baza-statystyczna/opracowania-wieloletnie/.

[31] K. J. Jakubski, *Analiza Strategii Cyberbezpieczeństwa Rzeczpospolitej Polskiej na lata 2017–2022, Fundacja Po.Int 2017,* https://fundacjapoint.pl/2017/05/analiza-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2017-2022/, [dostęp: 9.09.2017].

Konarska-Wrzosek V., *Kodeks Karny Komentarz,* Wolters Kluwer, Warszawa 2016.

Kosiński J., *Paradygmaty cyberprzestępczości*, Difin, Warszawa 2015.

Mroczek A., Sułkowska A., *Zabezpieczanie dowodu elektronicznego*, [w:] K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Sieciocentryczne bezpieczeństwo. Wojna, pokój i terroryzm w epoce informacji,* Difin, Warszawa 2014.

Skrzypczak J., *Polityka ochrony cyberprzestrzeni RP*, „Przegląd Strategiczny" 2014, nr 7.

Świecki D., *Kodeks Postępowania Karnego. Komentarz,* Wolters Kluwer Polska, Warszawa 2017.

Ziółkowska A., *Komentarz do art. 41 kodeksu karnego*, [w:] V. Konarska-Wrzosek, *Kodeks Karny. Komentarz*, Wolters Kluwer, Warszawa 2016.