Розділ 1

Теорія та історія держави і права; історія політичних та правових учень. Конституційне право; муніципальне право. Філософія права

UDC 340

A.I. Francuz
Bohater Ukrainy, Wybitny prawnik Ukrainy,
doktor nauk prawnych, profesor,
Kierownik departamentu dyscyplin państwowo-prawnych,
Uniwersytet ekonomii i prawa "KROK"

Dr Justyna Stadniczeńko
Adiunkt – Katedra Prawa Cywilnego
i Prawa Prywatnego Międzynarodowego,
Wydział Prawa i Administracji,
Wyższa Szkoła Finansów i Zarządzania w Warszawie,
Adwokat – Kancelaria Adwokacka z siedzibą w Opolu

Ochrona dziecka (dzieciństwa) przed negatywnym wpływem nowoczesnych technologii w polskim systemie prawnym. Zagadnienia wybrane

А.Й. Француз
Герой України, заслужений юрист України,
доктор юридичних наук, професор,
завідуючий кафедрою державно-правових дисциплін,
Університет економіки та права «КРОК»

Ю. Стадніченко
доктор юридичних наук,
асистент кафедри цивільного права та
міжнародного приватного права,
факультет права і адміністрації,
Університет фінансів і управління у Варшаві

Захист дитини (дитинства) від негативного впливу сучасних технологій у польській правовій системі. Вибрані теми

У статті досліджується питання захисту дитини (дитинства) від негативного впливу сучасних технологій у польській правовій системі.

Ключові слова: *захист дитини, дитинство, сучасні технології, польська правова система.*

А.И. Француз
Герой Украины, заслуженный юрист Украины,
доктор юридических наук, профессор,
заведующий кафедрой государственно-правовых дисциплин,
Университет экономики и права «КРОК»

Ю. Стадниченко
доктор юридических наук,
ассистент кафедры гражданского права
и международного частного права,
факультет права и администрации,
Университет финансов и управления в Варшаве

Защита ребёнка (детства) от негативного влияния современных технологий в польской правовой системе. Избранные темы

В статье исследуется вопрос защиты ребенка (детства) от негативного влияния современных технологий в польской правовой системе.

Ключевые слова: *защита ребенка, детство, современные технологии, польская правовая система.*

A. Frantsuz
Hero of Ukraine, Honored Lawyer of Ukraine,
Doctor of Law, Professor,
Head of the Department of State and Legal Disciplines,
"KROK" University
Justyna Stadniczeńko
Doctor of Law,
Assistant Professor – Department of Civil Law and
Private International Law,
Faculty of Law and Administration,
University of Finance and Management in Warsaw

Protection of the child (childhood) against the negative influence of modern technologies in the Polish legal system. Selected topics

The article examines the question of protection of the child (childhood) from the negative influence of modern technologies in the Polish legal system.
Keywords: *child protection, childhood, modern technologies, Polish legal system.*

Wprowadzenie

Dzieciństwo to okres pomiędzy niemowlęctwem a końcem dorastania i nie jest wyłącznie czyste i niewinne. Niebezpieczeństwo, ciekawość płciowości, fascynacja przemocą i grozą, horrorami, zaintrygowanie występkami dorosłych to normalne elementy dorastania, tak jak skłonność do buntu, zmienne nastroje, wyładowanie emocji oraz przekonanie, że rodzice, nauczyciele oraz inni dorośli przeważnie nic nie rozumieją (nie wiedzą) a jedynie „czepiają się". Ze względu na to, że dzieciństwo to okres niebezpieczny, podczas którego niedoświadczone dzieci dopiero się kształtują i są bezbronne, na rodzicielstwo składa się zarówno strach jak i miłość, które są nierozłącznie ze sobą związane. Rodzice z miłości opiekują się dziećmi, chcą żeby były bezpieczne, zdrowe, szczęśliwe oraz żeby wyrosły na ludzi dobrze przystosowanych, produktywnych i kochających życie. A jednocześnie spędza im sen z powiek wszystko, co może je tego pozbawić. Wiele czynników przyczynia się bezpośrednio do narażenia dzieci na niebezpieczeństwo. Jest to ważki zbiór zagadnień mający głęboki i daleko idący wpływ na dzieci. K. Goździewska[1] podaje, że „Naukowcy alarmują: pole elektromagnetyczne wytwarzane przez urządzenia bezprzewodowe jest groźne dla zdrowia, zwłaszcza dzieci. Coraz więcej krajów ogranicza dostęp do sieci Wi-Fi w szkołach i budynkach publicznych".

Eksperci apelują do Organizacji Narodów Zjednoczonych oraz Światowej Organizacji Zdrowia o wprowadzenie legislacji chroniącej obywateli przed nadmiernym promieniowaniem elektromagnetycznym, które zaliczane jest do największego energetycznego zanieczyszczenia na ziemi – wielokrotnie przekracza – naturalne poziomy. W Polsce cały czas urządzenia wykorzystujące technologie bezprzewodowe przyjmowane są jako dobrodziejstwo. W miastach trudno znaleźć przestrzeń od Wi-Fi – samorządy wręcz chlubią się powszechnym dostępem do sieci. Faktem jest, że na tle Europy słabo realizujemy Europejską Agendę Cyfrową, która nakłada na nas obowiązek zapewnienia 100 procentom obywateli szybkiego internetu o prędkości co najmniej 30 Mb/s, a w przypadku 50 procent

[1] K. Goździewska, Niewidoczni zabójcy /w/ Nasz Dziennik, Nr 194, 5642, 20-21 sierpnia 2016

obywateli nawet 100 Mb/s. Wyjściem ma być niestety internet przesyłany falami radiowymi, a nie światłowodem. Technologia Wi-Fi jest bowiem 40 razy tańsza od dużo zdrowsza dla organizacji człowieka drogi przesyłu sygnału internetowego za pomocą światłowodów.

Polska opinia publiczna niewiele może znaleźć informacji o wpływie pola elektromagnetycznego, jakie wytwarzają Wi-Fi czy stacje nadawcze – zarówno te duże jak i te małe znajdujące się w naszych laptopach, telefonach komórkowych, smartfonach, telewizorach, a także radiowych licznikach prądu wody. Emitują one do środowiska pole elektromagnetyczne o częstotliwościach od 30 kHz do 300 GHz. Dla przykładu funkcja Wi-Fi w mieszkaniu działa w oparciu o częstotliwość radiową w paśmie 2,4–2,5 GHz. Jest to pasmo wykorzystane w m.in. technice mikrofalowego podgrzewania żywności. Francja na początku 2015 roku przyjęła ustawę zakazującą stosowania Wi-Fi we wszystkich placówkach opiekujących się dziećmi poniżej 3 roku życia, ograniczyła także dostęp do mobilnego internetu w szkołach. Producenci telefonów komórkowych zostali zobowiązani do wyposażenia aparatów w zestawy słuchawkowe. Zakazano kierowania reklam telefonów komórkowych do dzieci poniżej 14 roku życia.

Zakaz używania sieci Wi-Fi i telefonów bezprzewodowych w szkołach i przedszkolach wprowadził austriacki departament zdrowia. Austriaccy lekarze stworzyli też przewodnik diagnozowania i leczenia osób dotkniętych „nadwrażliwością elektromagnetyczną". Specjalną kampanię mającą chronić dzieci przed polem elektromagnetycznym przygotował Cypr. Podobne kroki powzięły Niemcy. M. Kacprzak[2] „długotrwale korzystanie z internetu co prawda rozwija umiejętności wizualne, ale w tym samym czasie powoduje trudności w czytaniu ze zrozumieniem, która leży u podstaw zdobywania wiedzy analizy informacji, krytycznego myślenia i refleksji."/.../ „Obszary w mózgu, który zmieniają swe działanie pod wpływem długotrwałego używania internetu, odpowiedzialne są za zarządzanie emocji, uwagą, zdolnością skupienia i innymi funkcjami poznawczymi ponadto zaobserwowano, że u osób uzależnionych od internetu zachodzą analogiczne zmiany w mózgu jak u ludzi uzależnionych od alkoholu czy narkotyków." Podaje, że „Walter Isaacson w wydanej w 2011 roku biografii Steve'a Jobsa, genialny twórca multimedialnych gadżetów opatrzonych symbolem nadgryzionego jabłka, pozwalam swoim dzieciom korzystać z komputerów jedynie dwa razy w tygodniu nie dłużej niż dwie godziny. Jobs zdawał sobie sprawę lepiej niż wielu rodziców, że długotrwałe korzystanie sieje więcej spustoszenia w organizmie ludzkim zwłaszcza dziecka niż dobra."

Wszechobecny i ekspansywny marketing nastawiony na dzieci stosuje coraz bardziej bezwzględne i przebiegłe metody manipulacji ich kształtującymi się i wrażliwymi emocjami, sprzyja kompulsywnym zachowaniom i tumani niedojrzałe umysły pomocą, seksem oraz obsesyjnym konsumpcjonizmem oraz hedonizmem. Przed swoją potęgą i wpływy bogate państwa kształtują bezpośrednio i pośrednio politykę oraz praktykę e krajach biedniejszych i mniej rozwiniętych.

Społeczeństwo, które uchyla się od chronienia swoich najwrażliwszych członków od krzywdy i wyzysku, nawet kiedy może to zrobić i kiedy nie ma istotnych przeszkód – to naprawdę się „pogubiło". Nelson Mandela powiedział kiedyś „dusza społeczeństwa najgłębiej przejawia się w sposobie, w jaki traktuje ono dzieci".

Prawo międzynarodowe i ustawodawstwa krajowe uznało dzieci za osoby o szczególnych prawach i potrzebach, wymagające wyjątkowej ochronie.

W marketingu dziecięcym w przestępczości funkcjonującej w cyberprzestępczości wykorzystywane są szczególne cechy emocji młodych ludzi do których zaliczamy – miłość, skojarzona z opieką, uczuciem i romansem, strach skojarzony z przemocą, terrorem, horrorem, okrucieństwem, wojną, chęć zdobycia mistrzostwa wynikająca z dążenia do tego, by się uniezależnić od dorosłych, a także opanować nowe umiejętności (np. w grach komputerowych lub sieciowych). Ważne są wyobraźnia – narzędzie, które umożliwi im spełnienie marzeń w odrealnionym świecie fanta-

[2] M. Kacprzak, Niewidoczni zabójcy, op. Cit.

zji" – radzi Lindstrom – „i już jesteś do przodu"), humor („struny naciągane są do granic wytrzymałości, żartuje się z dorosłych i robi się szalone rzeczy" i wartość kolekcjonerska (zbieranie kart, odznak,znaczków i wizerunków postaci). Na koniec należy wspomnieć o efekcie lustra, pragnie naśladowania świata dorosłych. „Zamysł umożliwiający dzieciom odgrywanie roli dorosłych z pewnością spotka się z ich zainteresowaniem" – stwierdza Lindstrom. „Im się jest młodszym, tym bardziej chce się być starszym. (…) Dziewięciolatki chcą mieć 14 lat, żeby już mogły być zaliczane do grona prawdziwych nastolatków. Czternastolatki z kolei za nic mają nastolatki, bo chcą już prowadzić prawdziwe dorosłe życie"[3]. Skuteczny marketing dla dzieci i nastolatków wymaga jednak czegoś więcej niż granie na tych emocjach. Równie istotne, jak radzi Lindstrom, jest użycie właściwego medium. Dziś, kiedy „interaktywność jest wszystkim", marketerzy, chcąc skutecznie dotrzeć do dzieci, muszą przede wszystkim wziąć pod uwagę ich głębokie i trwałe zaabsorbowanie mediami interaktywnymi, takimi jak gdy, wirtualne światy i sieci społecznościowe.

Zdaniem specjalistów od gier psychologa G. Douglas nie jest tajemnicą, że „głównym wskaźników sukcesu" w tej branży jest takie ich projektowanie, żeby uzależniały. W świecie gier wystąpiła nowa tendencja – powiązanie ich z serwisami społecznościowymi co pogłębia ich wpływ na psychikę dzieci. Granie staje się bowiem jeszcze bardziej obsesyjne i uzależniające. Dla nastolatków i nieco młodszych dzieci drastycznych i agresywna treść ma nieotarty powab. Rozwijającą się psychikę, atakowaną przez „uaktywnione i zwielokrotnione id, przychodzące jak gdyby z wrogiego świata wewnętrznego", jak opisywał okres dojrzewania psychoanalityk E.Erikso, fascynuje przemoc, groza, okrucieństwo i seks, zwłaszcza kiedy rodzice wyrażają dezaprobatę.

Gry społecznościowe, wykorzystując prawdziwe emocje i stosunki między ludźmi, nadają graniu nowy wymiar, któremu trudno się oprzeć. Atrakcyjność gier przenosi się do uczestników z Facebooka.

Niezwykle niebezpieczne jest natężenie przestępczości w ramach rozwoju technologicznego w tym niewłaściwe wykorzystywanie danych osobowych, które są przetwarzane. Prawo nakłada obowiązki na tych, którzy chcą gromadzić lub wykorzystywać dane innych osób i przewiduje, że niezależny organ ochrony danych będzie monitorować poszanowanie wszystkich obowiązujących zasad. Społeczeństwo powinno umożliwić dzieciom rozwijanie indywidualnych charakterów, zapewnić im warunki rozkwitu, by mogły się stać „szlachetnymi i pięknymi przedmiotami kontemplacji", o których pisał Mill. „Natura ludzka nie jest maszyną zbudowaną według modelu i postawioną do wykonywania wyznaczonej pracy, lecz drzewem, które rośnie i rozwija się na wszystkie strony zgodnie z dążeniem sił wewnętrznych, które czynią je żywą istotą. (…) O człowieku, którego pragnienia i popędy są wyrazem jego natury (…) mówimy, że ma charakter. (…) Ludzkie istoty stają się szlachetnym i pięknym przedmiotem kontemplacji nie dzięki zacieraniu wszystkich przedmiotów kontemplacji nie dzięki zacieraniu wszystkich przymiotów indywidualnych w celu ich ujednostajnienia, lecz dzięki ich doskonaleniu i używaniu w granicach wyznaczonych przez prawo i interesy innych"[4].

Na tym powinno polegać dzieciństwo – tak uważano w czasie stulecia dziecka. Jednak na tak pojmowane dzieciństwo przypuszczono obecnie atak, ponieważ przemysł, przestępcy oraz korporacje bez ograniczeń wykorzystują bezbronność dzieci i lekceważą ich interesy. Należy jak najszybciej z tym skończyć ale najpierw trzeba to zjawisko zauważyć i zrozumieć.

I. Polskie regulacje prawne

Nasilenie globalizacji oraz rozwój nowych technologii na przestrzeni ostatnich kilku lat prowadzi do tego, że cyberprzestępczość jest coraz większym problemem. Sukcesywny rozwój społeczeństwa informa-

[3] M. Lindstom, P.B. Seybold, Dziecko reklamy. Dlaczego nasze dzieci lubią to co lubią, Przeł. A.M. Kawęca, Warszawa 2005, s.106

[4] J.S. Mill, O wolności, przeł. A. Kurlandzka, Warszawa 1999, s. 75

cyjnego zapoczątkował dynamiczne zmiany związane z wymianą informacji[5].

Rynek w świecie dla grupy dziecięcomłodzieżowej znajduje się na szczycie aktualnych trendów internetowych, obejmujących między innymi sieci społecznościowe, gry i wirtualne światy. Reklamodawcy, marketingowcy uznali, że przede wszystkim należy umieć dotrzeć do tej grupy przez środki masowego przekazu (telewizja, internet, itd.) bowiem tam spędza ona najwięcej czasu w porównaniu z innymi mediami.

Łatwo można zauważyć, iż rozwojowi cyberprzestępczości sprzyja specyficzny charakter sieci globalnej, który pozwala na częściową anonimowość sprawcy przestępstwa. Łatwość dostępu do sieci jest dodatkowym motorem napędzającym ich działanie.

Ilość użytkowników takich portali społecznościowych, jak Facebook i Twitter przewyższa wielkością kilka państw. Założenie, że wszyscy użytkownicy są przyjaźnie nastawieni jest nierealistyczne i niebezpieczne. Istnieje wiele przykładów cyberprzemocy i można je spotkać w Internecie każdego dnia, na „ścianach" portali społecznościowych, w komentarzach artykułów, blogów oraz w e-mailach a należą do nich: Wysyłanie dużych ilości wulgarnych emaili lub SMS-ów, zniesławienie na Twitterze, blogach i forach dyskusyjnych, podszywanie się pod innych na portalach społecznościowych, włamywanie się do urządzeń mobilnych w celu szpiegowania, kradzieży lub modyfikacji danych, kradzież tożsamości w celu zrujnowania reputacji ofiary.

Wszyscy korzystają z poczty elektronicznej, lecz niewielu wie, że jak korzystać z niej kulturalnie[6]. W zasadzie nie są znane zasady korzystania z niej, metody rozpoznawania e-mailowych fałszywek itp.

Dzieci z racji swojej łatwości przyswajania nowinek technologicznych (ang. breezy familiarity)[7], często są nazywane „cyfrowymi tubylcami" (ang. digital natives)[8]. Używają informacji inaczej niż ich starsi koledzy i koleżanki[9]. Coraz częściej korzystają z i tak ju,ż popularnych w swojej grupie wiekowej technologii. Już w 2011 roku ponad 75 % dzieci w Europie używało Internetu z przeróżnych powodów: od komunikowania się z rówieśnikami przez odbieranie różnych treści aż po granie w gry. Niektórzy tworzą własne treści w internecie np. pisząc bloga[10]. Wraz z upływem czasu, dzieci przebywają online coraz dłużej, poznają internet w coraz młodszym wieku i korzystają z niego w bardziej różnorodny sposób[11]. Zatem nic dziwnego, że to właśnie dzieci coraz częściej stają się rynkowym celem innowacyjnych praktyk przetwarzania danych. Udostępnione „selfie"z własnym świadectwem szkolnym jest już czymś powszechnym a każdy dzień przynosi coś nowego np. nowe aplikacje na do pomiaru wagi, tkanki tłuszczowej itp. czy smart watch, czyli inteligentne zegarki pozwalające rodzicom wiedzieć gdzie znajduje się ich dziecko[12]. Ludzie udostępniając swoje dane w internecie tracą kontrole nad ich kolejnym udostępnianiem czy przetwarzaniem i nie do końca są świadomi ryzyka związanego z udostępnianiem, przetwarzaniem oraz potencjalnym wpływem tego typu działań na ich życie obecne jak i przyszłe. Kiedy dane dotyczące dzieci

[5] W obliczu błyskawicznie zachodzących zmian w nowych technologiach w 2010 r. powstał Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011-2016. Ten obszerny dokument zawiera propozycje działań o charakterze prawno-organizacyjnym, technicznym i edukacyjnym, których celem jest zwiększenie zdolności do zapobiegania i zwalczania zagrożeń ze strony cyberprzestępców.

[6] S. Miller, E-mailowy savoir – viwre, Poznań 2003

[7] Sprawa American Libraries Association v. Pataki (1997) 969 F. Supp.160

[8] M. Prensky, Digital Natives, Digital Immigrants' (2001) 9 On the Horizon 5,1

[9] M. Prensky, Op.cit.

[10] S. Livingstone et al., Risks and Safety on the Internet: The Perspective of European Children London School of Economics and Political Science, London 2011, str 33,

[11] S. Livingstone (red.) EU Kids Online. Findings, Methods, Recommendations, London School of Economics and Political Science, London, 2015, str 6

[12] G. Gonzalez Fuster, GDPSR: we all need to work at it!, Better Internet for Kids (BIK) Bulletin 2016, str. 7

są przetwarzane, nie tylko zwiększą się istnienie ryzyka wyrządzenia im szkody, ale także te same dzieci narażone są na nowe jego rodzaje. Dlatego dzieci wymagają specjalnej ochrony. Dopiero niedawno prawo Unii Europejskiej zaczęło otwarcie dostrzegać i uwzględniać taką potrzebę. W ostatnim czasie zakończona (kwiecień 2016 roku) reforma ochrony praw danych osób wyraźnie uznaje konieczność zapewnienia specjalnego poziomu takiej ochrony dla grup szczególnie wrażliwych, między innymi właśnie dzieci. Preambuła do ogólnego rozporządzenia o ochronie danych podkreśla, że (…) szczególnej ochrony danych osobowych wymaga dzieci, gdyż mogą one być mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych. Taka szczególna ochrono powinna mieć zastosowanie przede wszystkim do wykorzystywania danych osobowych dzieci do celów marketingowych lub do tworzenia profili osobowych lub profili użytkownika oraz do zbierania danych osobowych dotyczących dzieci, gdy korzystają one z usług skierowanych bezpośrednio do nich (…)[13].

Należy zauważyć, że rozwój cyberprzestępczości doprowadził do pełnej modyfikacji narzędzi wykorzystywanych przez przestępców[14].

Szybki rozwój technologiczny, a tym samym ciągła potrzeba modyfikacji narzędzi informatycznych nastręcza licznych problemów. Dostawcy usług internetowych nierzadko stają się ofiarami ataków hakerskich. Odpowiedzialnością takich usługodawców jest więc zapewnienie odpowiedniego bezpieczeństwa swoich usług i produktów. Regulacje prawne w tym zakresie pozostają stale w tyle. Postęp technologiczny w obecnych czasach następuje w niewyobrażalnym tempie. Stworzenie praktycznych i użytecznych definicji legalnych stanie się dobrym punktem wyjściowym dla interpretacji przepisów. Właściwe ich zrozumienie zagwarantuje eliminację luk w zakresie cyberprzestępczości. Powstaną tym samym ujednolicone ramy prawne, które w pełni realizują postulat bezpieczeństwa prawnego i zapewnią ochronę informacji należących do każdego człowieka.

Cechą polskiej cyberprzestępczości jest jej bardzo duże zróżnicowanie zarówno pod względem liczby przestępstw stwierdzonych, jak i wskaźników natężenia przestępczości.

Warto zauważyć, że w polskim ustawodawstwie nie ma definicji legalnej takich pojęć jak „cyberprzestępczość" czy „przestępczość komputerowa". Obecnie w polskim porządku prawnym używana są definicje przygotowane przez organizacje unijne czy Interpol.

Analizując podstaw legislacyjnych ochrony praw dziecka w obowiązującym w Polsce systemie prawnym należy stwierdzić, iż fundamentalne znaczenie posiada treść postanowień zawartych w art 30 Konstytucji RP[15] z 1997 r. w którym zapisano między innymi: Przyrodzona i niezbywalna godność człowieka stanowi źródło wolności i praw człowieka i obywatela. Jest ona nienaruszalna, a jej poszanowanie i ochrona jest obowiązkiem władz publicznych. W art. 30 Konstytucja RP przedstawia najszersze ujęcie zasady i jest zarazem nakazem kierowanym do ustawodawcy.

Dziecko jest człowiekiem, który wymaga zapewnienia mu odpowiednich warunków do pełni osobowego rozwoju. Konstytucja zawiera katalog podstawowych praw i wolności obywatelskich, a także przepisy szczególne dotyczące bezpośrednio praw dziecka. Nie należy zapominać, iż prawa dziecka to prawa człowieka, który jest chroniony od momentu jego poczęcia. Ponadto w art. 72 ust 1 wysłowione zostało, iż „Rzeczpospolita Polska zapewnia ochronę praw dziecka. Każdy ma prawo żądać od organów władzy publicznej ochrony dziecka przed

[13] Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 keitnia 2016 roku w sprawie ochrony danych osobowych osób fizycznych w zakresie przetwarzania danych osobowych i swoboddnego przepływu tych danych uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych) 2016 Dz.U.L.119/1

[14] K.Gienas, Cyberprzestępczość, Jurysta 2003 nr 12 s. 9-10

[15] Konstytucja RP z dnia 2 kwiatnia 1997, Dz. U. z 1997 r. Nr 78, poz. 483, z późn. zm.

przemocą, okrucieństwem, wyzyskiem i demoralizacją”[16]. Przepisy Konstytucji RP określają również procedurę realizacji tych praw dziecka. Mianowicie w toku ustalania praw dziecka organy władzy publicznej oraz osoby odpowiedzialne za dziecko są obowiązane do wysłuchania i w miarę możliwości uwzględnienia zdania dziecka. Sprawia to, iż głos i zdanie dziecka powinno być ważne dla organów władzy publicznej. W ten sposób dziecko z biernego podmiotu swoich własnych praw staje się aktywnym członkiem życia społecznego.

Wewnętrzne regulacje prawne, dotyczące krzywdzenia dzieci, są często konsekwencją ratyfikacji dokumentów międzynarodowych, zdarza się, że swoją innowacyjnością wyprzedzają międzynarodowe akty prawne, częściej jednak, m.in. w krajach Europy Wschodniej, nie nadążają za światowymi standardami.

Taka sytuacja miała długi czas miejsce w odniesieniu do norm polskiego kodeksu karnego odnośnie prawnego zakazu posiadania pornografii dzieciPrawnokarna ochronę dzieci przed cyberprzestępczością seksualną polski Kodeks karny z 1997 roku zawiera regulacje w a) art 200 a kk, b) art 200 b kk oraz c) 202 kk.

a) po pierwsze przestępstwa uwodzenia dziecka za pomocą systemu teleinformatycznego (*grooming*) (art. 200a § 1 i 2 kk), dostosowując ustawodawstwo polskie do standardów Konwencji z Lanzarote, ustawą z 5 listopada 2009 roku[17] wprowadzono do Kodeksu karnego art. 200a § 1 i 2 sankcjonujący przestępstwo polegające na nagabywaniu dziecka w celu wykorzystania seksualnego (*grooming*). Jest to przestępstwo o charakterze umyślnym, które można popełnić wyłącznie z zamiarem bezpośrednim. Karze podlega zachowanie sprawcy polegające na oddziaływaniu na psychikę, w tym na procesy decyzyjne, osoby małoletniej poniżej 15 – go roku życia w celu popełnienia na niej przestępstwa zgwałcenia, doprowadzenia do poddania się czynności seksualnej lub jej wykonania. Sprawca osiąga ten efekt poprzez wprowadzenie małoletniego w błąd (czyli wywołanie w nim fałszywego wyobrażenia o jakimś stanie rzeczy), wykorzystanie sytuacji, w której pozostaje on w błędzie (tzw. oszustwo bierne) lub brak mu dostatecznego rozeznania w sytuacji, a także przy użyciu groźby bezprawnej. Przykładem błędu może być niezgodne z rzeczywistością przekonanie dziecka o wieku, płci lub tożsamości sprawcy. Skutek w postaci spotkania z dzieckiem i popełnienia przestępstwa z art. 197 § 3 lub art. 200 k.k. nie jest konieczny, aby zostały wypełnione znamiona przestępstwa *groomingu*.

Przy interpretacji znamion: „system teleinformatyczny” i „sieć telekomunikacyjna” należy sięgnąć do przepisów ustawy z dnia 18 lipca 2002 roku o świadczeniu usług drogą elektroniczną oraz ustawy z 16 lipca 2004 roku – Prawo telekomunikacyjne[18]. Na tej podstawie za system teleinformatyczny należy uznać: „zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania, zapewniający przetwarzanie, a także wysyła nie i odbieranie danych poprzez sieci telekomunikacyjne za pomocą właściwego dla danego rodzaju sieci urządzenia końcowego”. Siecią telekomunikacyjną są zaś: „systemy transmisyjne oraz urządzenia komunikacyjne lub przekierowujące, a także inne zasoby, które umożliwiają nadawanie, odbiór lub transmisję sygnałów za pomocą przewodów, fal radiowych, optycznych lub innych środków wykorzystujących energię elektromagnetyczną, niezależnie od ich rodzaju”. Kwestią problematyczną pozostaje wspomniane wcześniej wprowadzenie możliwości tzw. prowokacji policyjnej, czyli czynności operacyjno–rozpoznawczych wobec sprawców przestępstwa z art. 200a k.k. Przy założeniu, że czynności te miałyby polegać na próbie kontaktu pedofila za pośrednictwem sieci z funkcjonariuszem udającym dziecko, nie stanowi to dowodu popełnienia przestępstwa *groomingu*, bowiem do zna mion czynu należy kontakt z dzieckiem poniżej 15 – go

[16] S.L. Stadniczeńko, Ochrona dziecka przed przemocą, okrucieństwem, wyzyskiem, demoralizacją, zaniedbaniem oraz innym złym traktowaniem /w/ Prawa dziecka po przystapieniu do Unii Europejskiej (red.) M. Potapowicz, M. Krauzowicz, P. Przybylski.

[17] Dz.U. Nr 206, poz. 1589.

[18] tj. Dz. U. z 2014 r. poz. 243.

roku życia, a nie z osobą podszywającą się pod dziecko[19].

b) Po drugie przestępstwa propagowania lub pochwalania zachowań o charakterze pedofilskim (art. 200b kk). Za znaczący krok w kierunku prawnokarnej ochrony dzieci przed przestępczością na tle seksualnym należy też uznać wprowadzenie art. 200b k.k. penalizującego publiczne propagowanie lub pochwalanie zachowań o charakterze pedofilskim[20]. Jak zauważa bowiem jeden z komentatorów nowelizacji, zjawisko pedofilii, jako „godzące w pod stawowe dla każdego społeczeństwa wartości i dobra jakim jest prawidłowy i niezakłócony rozwój fizyczny i psychiczny dziecka", zasługuje na zastosowanie szczególnych środków w celu jego zwalczania[21].

c) Po trzecie przestępstw związanych z prezentowaniem, rozpowszechnianiem, produkowaniem, uzyskiwaniem lub posiadaniem treści pornograficznych za pośrednictwem Internetu (art. 202 kk), artykuł 202 § 1–4b k.k. reguluje przestępstwa związane z pornografią, które można popełnić przy użyciu komputera niepodłączonego do sieci, który pełni jedynie funkcję nośnika treści i umożliwia ich odtwarzanie, a także odnosi się do tzw. pornograficznych przestępstw w cyberprzestrzeni[22], które wymagają przekazu informacji za pomocą Internetu. Oprócz zakazu dotyczącego publicznej prezentacji treści pornograficznych osobom dorosłym, które sobie tego nie życzą, art. 202 § 2 k.k. za przestępstwo uznaje prezentowanie takich treści małoletniemu poniżej lat 15. Należy zaznaczyć, że przepis ten sankcjonuje prezentowanie treści pornograficznych konkretnej, dającej się zindywidualizować osobie, nie dotyczy zatem sytuacji, kiedy małoletni – przeglądając różnorakie strony internetowe – natyka się na linki do stron pornograficznych. Znamiona przestępstwa z art. 202 § 2 k.k. spełnia natomiast przesyłanie takiej osobie materiałów pornograficznych na indywidualny adres poczty elektronicznej, jeżeli sprawca zdaje sobie sprawę, że należy on do osoby, która nie ukończyła 15 lat. W redakcji przepisów odnoszących się do pornografii zastosowano pojęcie „treści pornograficznych", co pozwoliło na objęcie nim również elektronicznych form przekazu, w oderwaniu od materialnego nośnika, jak przewidywała regulacja z 1969 roku używając pojęcia „przedmiotów o charakterze pornograficznym"[23]. Na mocy nowelizacji z 24 października 2008 roku[24], do treści pornograficznych zaliczane są wszystkie formy cyberpornografii dziecięcej, a więc także wirtualna pornografia dziecięca (art. 202 § 4b k.k.). W porównaniu do art. 202 § 2 oraz kwalifikowanych przestępstw dotyczących pornografii dziecięcej z udziałem małoletniego poniżej lat 15 (art. 202 § 4 i art. 202 § 4a k.k.), art. 202 § 3 oraz art. 202 § 4b k.k. posługują się wyłącznie określeniem „małoletni", co sugeruje rozszerzony zakres ochrony obejmujący osoby poniżej 18. roku życia lub jedynie wirtualne wizerunki takich osób. Przy niezmienionej treści art. 202 § 4a k.k. dochodzi w tym miejscu do niespójności, bowiem zgodnie z aktualnym brzmieniem przepisów sankcjonowane jest posiadanie i przechowywanie wirtualnej pornografii dziecięcej z udziałem małoletniego do 18-go roku życia, natomiast analogiczne wizerunki rzeczywistych dzieci są zakazane w przypadku, gdy dziecko nie ukończyło lat 15. Kolejnych problemów związanych z przyjętymi rozwiązaniami prawnymi nastręcza przypisanie sprawstwa w postaci posiadania i przechowywania pornografii dziecięcej. Profesor A. Adamski zwraca uwagę, iż w świetle obowiązującej regulacji czyn określony w art. 202

---

[19] *P. Siemkowicz, Przestępstwa o charakterze pedofilskim i przeciwko wolności seksualnej popełniane poprzez Internet, w ujęciu polskiego kodeksu karnego*, e-Czasopismo Prawa Karnego i Nauk Penal nych 2011, nr 7„ s. 18.

[20] Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw, Dz.U. Nr 206, poz. 1589.

[21] P. Siemkowicz, *Przestępstwa..., op. cit.,* s. 19.

[22] J. Warylewski, *Pornografia w Internecie – wybrane zagadnienia karnoprawne*, Prokuratura i Prawo 2002, nr 4, s. 52.

[23] P. Siemkowicz, Przestępstwa..., op. cit. s. 17

[24] Ustawa z dnia 24 października 2008 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, Dz.U. Nr 214, poz. 1344.

§ 4 oraz 4b k.k. popełniają także przedstawiciele organów ścigania oraz biegli, którzy gromadzą i przechowują tego typu materiały w związku z prowadzeniem czynności śledczych lub w celach dowodowych w ramach postępowania sądowego[25]. W podobnej sytuacji znajdują się osoby, które nie zdają sobie sprawy, że na twardym dysku ich komputera znajdują się zapisy z pornografią dziecięcą. Jest to możliwe szczególnie w przypadkach, gdy nabyły komputer używany, bowiem umieszczenie plików w koszu systemu operacyjnego oraz usunięcie ich spośród plików jawnych nie wyłącza możliwości odzyskania tego typu zapisów za pomocą programów używanych chociażby przez techników kryminalistyki w celu odzyskiwania utraconych danych[26].

Przestępczość komputerowa od początku towarzyszyła rozwojowi nowoczesnych technologii, stopniowo zyskując na znaczeniu w policyjnych statystykach. O ile początkowo kwestia ta pozostawała raczej problemem marginalnym, o tyle pod koniec XX wieku, komputery powszechnie były już wykorzystywane jako narzędzia służące do dokonywania czynów zabronionych. Pochodną takiego stanu rzeczy, powstały nowe przestępstwa (np. sabotaż komputerowy – art. 269 k.k.), lecz przede wszystkim powstały całkowicie nowe formy popełnienia znanych już czynów zabronionych.

Znamiennym znakiem czasu stanowią policyjne przeszukania, których najważniejszym uczestnikiem jest często informatyk śledczy, gwarantujący prawidłowe zabezpieczenie materiału dowodowego (komputery, telefony komórkowe, karty pamięci).

W przypadku cyberprzemocy w stosunku do dzieci, czyli osób poniżej 18 roku życia, wszystkie działania prawne muszą realizować rodzice lub opiekunowie prawni. Nie jest możliwe dochodzenie odpowiedzialności prawnej dziecka pokrzywdzonego cyberprzemocą bez współpracy z rodzicami.

Niezależnie od formy cyberprzemocy, jeżeli podejrzanym – sprawcą cyberprzemocy jest osoba poniżej 17 roku życia, działania w sprawie realizuje Sąd rodzinny właściwy ze względu na miejsce pobytu sprawcy cyberprzemocy. Każdy, dowiedziawszy się o popełnieniu przestępstwa ściganego z urzędu, ma społeczny obowiązek zawiadomić o tym prokuratora lub policję. Instytucje państwowe i samorządowe, które w związku ze swoją działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są zobowiązane niezwłocznie zawiadomić o tym prokuratora lub policję zgodnie z treścią art. 304 § 1 i 2 k.p.k.

Zgodnie z art 47 Konstytucja RP każdy ma prawo do ochrony prawnej życia prywatnego, rodzinnego, czci i dobrego imienia oraz do decydowania o swoim życiu osobistym.

Naruszenie dóbr osobistych, a w szczególności nazwiska lub pseudonimu i wizerunku oraz czci czyli działania polegające np. na umieszczenie zdjęcia lub filmu przedstawiającego kogoś na stronie internetowej, na blogu, w serwisie społecznościowym itp., rozesłanie zdjęcia przedstawiającego kogoś lub filmiku z czyimś udziałem e-mailem, telefonem komórkowym może prowadzić do odpowiedzialności zarówno karnej jak i cywilnej.

Kodeks cywilny[27] w art 23 określa, iż dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach. Natomiast w art. 24 § 1 kc zostało stwierdzone, iż ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba, że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie.

[25] A. Adamski, *Karnoprawna ochrona dziecka w sieci Internet,* Prokuratura i Prawo 2003, nr 9, s. 69.

[26] P. Siemkowicz, *Przestępstwa...,op. cit.,* s. 11.

[27] Kodeks cywilny z dnia 23 kwietnia 1964 r. t.j. Dz. U. z 2016 r. Poz. 380 z późn. zm.

Na zasadach przewidzianych w kodeksie cywilnym można żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny, a w § 2 kc dodaje, że jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych. Jedną z najpopularniejszych form cyberprzemocy jest właśnie wykorzystywanie czyjegoś wizerunku.

W rozdziale XXXIII Kodeksu Karnego[28] zatytułowanym „Przestępstwa przeciwko ochronie informacji" odnajdujemy szereg przepisów dotyczących czynów zabronionych. Próbą stworzenia jednolitego katalogu przestępstw internetowych zajęli się teoretycy i praktycy. Począwszy od kryminologów, a skończywszy na organizacjach pozarządowych.

Jednym z rodzajów cyberprzemocy jest naruszenie czci (zniesławienie, znieważenie) czyli zachowania uwłaczające czyjejś godności, stanowiące przejaw lekceważenia oraz pogardy, znieważenie drugiej osoby w Internecie lub przy użyciu innych technologii komunikacyjnych, pomówienie (oszczerstwo) o takie postępowanie lub właściwości, które mogą daną osobę poniżyć w opinii publicznej, np. umieszczenie wizerunku osoby w celu jej ośmieszenia np. na stronie internetowej, na blogu, w serwisie społecznościowym, rozesłanie e-mailem lub za pomocą telefonu komórkowego, tworzenie kompromitujących i ośmieszających stron internetowych, blogów, fałszywych kont i profili w serwisach społecznościowych.

Są to przestępstwo zniesławienia lub zniewagi opisane w kodeksie karnym w art. 212 i art. 216, w tym przypadku do ochrony dziecka rodzic powinien wykorzystać drogę karną, oba te przestępstwa są prywatnoskargowe, co oznacza, że osoba pokrzywdzona lub jej przedstawiciel prawny muszą sformułować prywatny akt oskarżenia

Kolejnym takim przestępstwem jest włamanie (art 267 kk oraz 268a kk) do miejsca w Internecie strzeżonego hasłem lub innym zabezpieczeniem np. Włamania na konto e-mailowe, profil w serwisie społecznościowym. Przez włamanie rozumiemy taką sytuację, gdy bezprawnie zostaje przełamane w Internecie zabezpieczenie: hasła, kody dostępu, itp. Włamanie na czyjeś konto jest kolejną formą cyberprzemocy, gdyż godzi w ważne dla dzieci prawo do prywatności.

Zgodnie ze stanowiskiem P. Kardasa[29] samo przełamanie zabezpieczeń oraz wdarcie się przez hackera do systemu komputerowego, przy czym nie jest tutaj istotny faktyczny cel działania sprawcy, a w szczególności czy rzeczewiście wejdzie on w posiadanie informacji zgromadzonych w tym systemie, lecz istotne jest samo narażenie zgromadzonych w systemie informacji i danych na niebezpieczeństwo.

Wąską interpretację art. 267 § 1 kk w jego brzmieniu sprzed przedmiotowej nowelizacji, przedstawiał natomiast W. Wróbel[30] uznając, że do odpowiedzialności za przestępstwo hackingu z art. 267 § 1 kk konieczne jest spełnienie dwóch niezależnych od siebie warunków, a mianowicie, że sprawca uzyskał dostęp do systemu komputerowego przełamując specjalne zabezpieczenie oraz, że następnie uzyskał dodatkowo znajdujące się w tym systemie informacje, które musiały być różne od treści hasła zabezpieczającego dostęp do systemu[31].

Grożenie komuś przy użyciu narzędzi dostępnych w Internecie jest wśród dzieci o tyle popularne, o ile wiąże się z poczuciem anonimowości i bezkarności. Młodzi inter-

[28] Ustawa z dnia 6 czerwca 1997 r. Kodeks karny., Dz.U.1997.88.553

[29] P. Kardas, Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych, Rok IV, 2000 r., z. 1, s. 60.

[30] W. Wróbel, Przestępstwa przeciwko ochronie informacji, Rzeczpospolita, nr 206 z 03.09.1993 r.

[31] W. Wróbel, Uwagi wprowadzające do Rozdziału XXXIII Kodeksu Karnego „Przestępstwa przeciwko ochronie informacji", w G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska-Kardas, P. Kardas, P. Majewski, M. Rodzynkiewicz, M. Szewczyk, W. Wróbel, A. Zoll, Kodeks Karny. Część szczególna. Komentarz, t. II, Kraków 1999 r., s. 968–969.

nauci często nie zdają sobie sprawy z tego, że istnieje możliwość identyfikacji nadawcy danego komunikatu, że nie pozostaną bezkarni tylko dlatego, że w Internecie nikt ich nie znajdzie. Policja posiada specjalistyczne narzędzia, które umożliwiają identyfikację i dotarcie do twórców niedozwolonych treści. Należy pamiętać, iż grożenie komuś popełnieniem przestępstwa (np. pozbawieniem życia) przez Internet, kierowanie do dziecka, za pomocą narzędzi dostępnych w Internecie, gróźb w celu zmuszenia go do określonego działania, w taki sposób, że groźba ta wzbudza obawę, że zostanie popełniona jest przestępstwem uregulowanym w art 190 kk.

Złośliwe niepokojenie jakiejś osoby w celu dokuczenia jej poprzez wykorzystanie Internetu czy wielokrotne powtarzanie jakiegoś działania w Internecie skierowanego na jakąś osobę wbrew jej woli np wielokrotne wysyłanie komuś w Internecie lub przy użyciu telefonu komórkowego niechcianych lub uprzykrzających informacji, obrazów, linków, zwłaszcza, gdy dokonuje się tego korzystając z różnych form internetowej komunikacji naraz, stanowi wykroczenie z art 107 kodeksu wykroczeń.

Często również można spotkać się z używaniem w Internecie wulgarnych zwrotów (w miejscach dostępnych powszechnie, czyli nie wymagających np. znajomości hasła i logowania się), umieszczaniem w Internecie nieprzyzwoitego zdjęcia lub rysunku (w miejscach dostępnych powszechnie) co stanowi wykroczenie z art 141 kodeksu wykroczeń.

Zajmując się tematyką cyberprzestępczości warto również zwrócić uwagę na szeroko pojętą ochroną informacji, a w szczególności ochroną danych osobowych. Nie ulega wątpliwości, że wdrożenie niezbędnej dokumentacji oraz przeprowadzenie szkoleń wydaje się kluczem do sukcesu. Należy jednak pamiętać, że nawet odpowiednie procedury czy nowoczesne zabezpieczenia systemów informatycznych nie ochronią informacji jeśli zawiedzie czynnik ludzki. Szczególnie w tym kontekście warto pamiętać o sukcesywnym poszerzaniu świadomości pracowników z zakresu bezpieczeństwa ochrony informacji. Ochrona danych osobowych w dzisiejszych czasach jest szczególnie ważna i brak dbałości w tym zakresie generuje niezliczone skutki nie tylko w sferze prawnej.

Niska wykrywalność cyberprzestępstw wynika niestety z przyzwolenia społecznego. Niewiele osób nie zdaje sobie sprawę z powagi sytuacji i wiele osób kwalifikuje tego typu przestępstwa jako czyn o niskim stopniu społecznej szkodliwości. Uważają, że przestępstwa komputerowe nie powinny stać się przedmiotem zainteresowania i wzmożonej kontroli ze strony organów ścigania i przestępcy czują się bezkarni. Takie przekonanie jest błędne i bardzo szkodliwe dla bezpieczeństwa każdego człowieka – dziecka.

II. Nowe technologie wyzwaniem dla ochrony prywatności, ochrony danych osobowych

Nowe technologie są źródłem nowych wyzwań dla ochrony prywatności. Coraz częściej i więcej komunikujemy się, uczymy się, bawimy, pracujemy korzystając z technologi a jednocześnie coraz bardziej są zagrożone nasze dane osobowe.

Prywatność zawsze odgrywa kluczową rolę w funkcjonowaniu współczesnych demokracji i została uznana za jedno z praw człowieka. Oprócz prawa do prywatności przysługuje także prawo do ochrony danych osobowych. Prawo to traktowane jest jako prawo podstawowe we współczesnych społeczeństwach z powodu tragicznych skutków, jakie niewłaściwe używanie może spowodować. Za dane szczególnie chronione uznane są dane, które odnoszą się do poglądów politycznych, religijnych, zdrowia, pochodzenia czy życia seksualnego. Tego rodzaju informacje objęte są szczególną ochroną, aby uniknąć dyskryminowania ludzi ze względu na powyższe kwestie, aby zapobiec jakiejkolwiek stygmatyzacji i aby pozwolić wszystkim ludziom, aby te dane były tak prywatne jak oni sami sobie tego życzą.

Prywatność polega na ochronie przez osoby swoich danych oraz osobistych zwyczajów, zachowań i nieujawnianie ich publicznie. Prywatność to także możliwość „bycia sobą“ i szansa na życie zgodnie z własnymi preferencjami, kształtowanie własnego życia zgodnie ze swoją wolą, prywatność zatem to możliwość odpierania prób naruszenia

swojej sfery prywatności przez innych tzn. Rodziców, przyjaciół, nauczycieli, państwo. Należy mieć na uwadze fakt, że prawa te są wymienione w Karcie Praw Podstawowych Unii Europejskiej – i to z racji ich ogromnego znaczenia dla funkcjonowania społeczeństwa demokratycznego. Uczenie o ochronie danych i prywatności nie powinno ograniczać się do zapewnienia „bezpieczeństwa" dzieciom. Musi ono także zapewniać, że będą one świadome swoich praw i gotowe ich bronić.

W Polsce od 2009 roku w programie skierowanym do szkół pt. *Twoje dane – Twoja sprawa,* który cieszył się powodzenie i zainteresowaniem wśród nauczycieli i dotyczył realizacji edukacji o ochronie danych osobowych i prywatności., ponieważ stanowią część umiejętności cyfrowych, które są fundamentem wiedzy XXI wieku i elementarnym warunkiem rozwoju nowoczesnych społeczeństw. Umiejętności cyfrowe są obecnie kluczem do aktywności społecznej służąc rozwijaniu kreatywności, innowacji i przedsiębiorczości.

Głównym celem tego programu realizowanego przez Głównego Inspektora Ochrony Danych Osobowych od lat jest poszerzanie oferty edukacyjnej ośrodków doskonalenia nauczycieli, szkół wszystkich poziomów poprzez wprowadzenie treści dotyczących ochrony danych osobowych oraz prawa do prywatności. Jednym z etapów programu jest szkolenie kadry pedagogicznej szkół i placówek doskonalenia nauczycieli raz wyposażenie ich w materiały edukacyjne zawierające między innymi informacje dotyczące zasad ochrony danych osobowych oraz scenariusze lekcji, a tym samym przygotowanie nauczycieli do kształtowania świadomych, odpowiedzialnych i otwartych postaw wśród uczniów. Innym elementem programu jest przeprowadzenie w szkołach i placówkach doskonalenia nauczycieli zajęć związanych z tematyką ochrony danych osobowych oraz opracowanie autorskich scenariuszy lekcji orz przygotowanie raportów ewaluacyjnych dotyczących działań podjętych w trakcie programu.

Realizowany ten program pod auspicjami GIODO pozwolił jemu na przeniesienie tego pomysłu na szczebel europejski – regionalny. Powstała koncepcja projektu europejskiego ARCADES. Wynikiem powyższego była propozycja projektu ARCADES złożona do Komisji Europejskiej w marcu 2014 roku w ramach programu Prawa Podstawowe i Obywatelstwo, zarządzanego przez Dyrekcję Generalną do spraw Sprawiedliwości. Została oceniona w lipcu 2014 roku i otrzymała dotację na działania dla czterech partnerów – Biura Generalnego Inspektora Ochrony Danych Osobowych jako koordynatora projektu, Rzecznika Informacji Republiki Słowenii, Krajowego Organu Ochrony Danych i Wolności Informacji na Węgrzech oraz Grupy Badawcze do spraw Prawa, Nauki, Technologii i Społeczeństwa na Vrije Universiteit Brussel w Belgii. Konsorcjum projektowe zostało dobrane uwzględniając doświadczenie każdego z partnerów w tworzeniu pomocy naukowych dla szkół. Szczególną rolę szkół w procesie edukowania dzieci i młodzieży na temat funkcjonowania w społeczeństwie oraz bezpiecznego poznawania cyfrowego świata dostrzegli także autorzy raportu Eurobarometru z 2008 roku.

Partnerzy projektu ARCADES w pierwszej kolejności dokonali podsumowania istniejącej wiedzy dotyczącej kształcenia w zakresie ochrony danych osobowych i prywatności w szkołach w Unii Europejskiej[32]. Raport zawiera zestaw podstawowych zasad ochrony danych osobowych i prywatności, a także przykłady materiałów i inicjatyw skierowanych do nauczycieli i uczniów, przedstawiając główne trendy w procesie nauczania o danych osobowych oraz przykłady najlepszych praktyk w tym zakresie.

W Warszawie w 2013 roku podczas 35 Międzynarodowej Konferencji Rzeczników Ochrony Danych i Prywatności przyjęto Rezolucję w sprawie edukacji cyfrowej dla wszystkich[33], w której wezwano organy ochrony danych do zwiększenia zaangażowania w działania edukacyjne skierowane

[32] G. Gonzales Fuster, P. De Hert, D. Kloza, Deliverable 1:1, State-of-the-Art Report on Teaching Privacy and Personal Data Protection at School in the European Union, ARCADES, marzec 2015

[33] https://icdppc.org/wp-content/uploads/2015/02/Digital-education-resolution.pdf> dostęp, 25.10.2016

do ogółu społeczeństwa, które mają pomóc obywatelom stać się świadomymi i odpowiedzialnymi podmiotami w społeczeństwie cyfrowym, którzy potrafią skutecznie korzystać ze swoich praw i znają swoje obowiązku w tym obszarze.

W ramach tych działań rezolucja nałożyła na Międzynarodową Grupę Roboczą ds Ochrony Danych i Edukacji Cyfrowej zadanie wdrożenia rocznych priorytetowych Planów Działania, takich jak „Rozwój pakietu szkoleniowego mającego na celu przeszkolenie trenerów w zakresie ochrony danych i prywatności" oraz „Stworzenie platformy internetowej do dzielenia się treściami i materiałami edukacyjnymi w zakresie edukacji cyfrowej" dla zainteresowania swoich głównych celów operacyjnych: obejmują one po pierwsze – promowanie edukacji w zakresie prywatności jako elementu programów nauczania kompetencji cyfrowych, po drugie przyczynianie się do szkolenia przyszłych osób szkolących przez organizowanie albo wkład w „doskonalenie zawodowe personelu szkolącego" w zakresie ochrony danych osobowych i prywatności.

Kwestie dotyczące bezpieczeństwa online dyktują nacisk na sposoby zapobiegania ryzyka w sieci a tym samym na trzymaniu dzieci z dala od zagrożeń, w odróżnieniu od wyjaśnienia im, że mają one pewne prawa podstawowe i że mogą domagać się przestrzegania pewnych zobowiązań dotyczących przetwarzania ich danych osobowych.

Podsumowanie

Nie ma wątpliwości, że technologia ma ogromny wpływ na współczesne społeczeństwo i jego rozwój. Nie ma także wątpliwości do tego co do tego, że nowe pokolenie czuje się znacznie swobodniej w świecie nowych technologii. Dziecko ma prawo do uzyskania każdej informacji której potrzebuje. Może korzystać miedzy innymi z zasobów internetu i innych technologii. Dziecko jednak należy chronić przed treściami dla niego nie przeznaczonymi i negatywnie wpływającymi na jego holistyczny rozwój.

Istnieją różne formy zabezpieczeń, lecz dzieci a zwłaszcza młodzież wykazują zdumiewająca umiejętność łamania ich ale nie znaczy to, dorośli nie mają ich wprowadzać i korzystać w interesie dobra dziecka. Oczywiście same zabezpieczenia nie wystarczą, konieczna jest efektywna edukacji i rozmowa z dzieckiem. Korzyści płynące z korzystania z nowoczesnych technologii łączą się jednocześnie ze znacznymi zagrożeniami dla praw jednostki w tym ochrony danych i prywatności. Umiejętność zarządzania informacjami i umiejętności cyfrowe staja się niewątpliwie niezbędne dla młodego pokolenia, dlatego misjom organów ochrony danych osobowych jak i organów ochrony praw dziecka jest zapewnienie, że dzieci i młodzież będą odpowiednio przygotowani do wyzwań jakie stawia nowa technologia i nie tracić tym samym korzyści płynących z używania tych technologii. W Polsce w ostatnich latach Rzecznik Praw Dziecka jak i Główny Inspektor Ochrony Danych Osobowych w podejmowanych przez siebie działaniach stawiali edukacji dzieci i młodzieży jako priorytet, dając temu wyraz poprzez szereg realizowanych inicjatyw i petycji do odpowiednich organów.

Często jest tak, że to szkoła jest pierwszym miejscem, gdzie dzieci i młodzież zgłaszają przypadki naruszenia ich prywatności stąd też na nauczycielach i rodzicach spoczywa obowiązek udzielenia odpowiedniej im pomocy oraz zabezpieczenia ochrony praw dziecka.

Zarówno sam fakt istnienia nowoczesnej technologii w tym cyberprzestępczości, problemów prywatności jak i poziom ich istotności są często niedoceniane. Dzieci są wrażliwe i podatne na niebezpieczeństwa przede wszystkim z powodu niewystarczającej świadomości zagrożeń w ogóle a w szczególności wynikających z nowych technologii i dlatego też zasługują na specjalną ochronę, która winna być permanentnie doskonalona.

Literatura

1. Adamski A., Cyberprzestępczość – aspekty prawne i kryminologiczne, Studia Prawnicze – Kwartalnik, nr 4/2005,
2. Adamski A., Karnoprawna ochrona dziecka w sieci Internet, Prokuratura i Prawo 2003, nr 9.
3. Gienas K., Cyberprzestępczość, Jurysta 2003 nr 12.

4. Gonzalez G. Fuster, GDPSR: we all need to work at it!, Better Internet for Kids (BIK) Bulletin 2016,

5. Gonzales G. Fuster, P. De Hert, D. Kloza, Deliverable 1:1, State-of-the-Art Report on Teaching Privacy and Personal Data Protection at School in the European Union, ARCADES, marzec 2015.

6. Goździewska K., Niewidoczni zabójcy /w/ Nasz Dziennik, Nr 194, 5642, 20-21 sierpnia 2016.

7. Kacprzak M., Niewidoczni zabójcy, Nasz Dziennik, 2016 nr 194.

8. Kardas P., Prawnokarna ochrona informacji w polskim prawie karnym z perspektywy przestępstw komputerowych. Analiza dogmatyczna i strukturalna w świetle aktualnie obowiązującego stanu prawnego, Czasopismo Prawa Karnego i Nauk Penalnych, Rok IV, 2000 r., z. 1,

9. Kardas P., Majewski P., Rodzynkiewicz M., Szewczyk M., Wróbel W., Zoll A., Kodeks Karny. Część szczególna. Komentarz, t. II, Kraków 1999 r.

10. Lindstom M., Seybold P.B., Dziecko reklamy. Dlaczego nasze dzieci lubią to co lubią, Przeł. A.M. Kawęca, Warszawa 2005,

11. Livingstone S., Risks and Safety on the Internet: The Perspective of European Children London School of Economics and Political Science, London 2011.

12. Livingstone S.(red.) EU Kids Online. Findings, Methods, Recommendations, London School of Economics and Political Science, London, 2015.

13. Mill J.S., O wolności, przeł. A. Kurlandzka, Warszawa 1999.

14. Miller S., E-mailowy savoir – viwre, Poznań 2003.

15. Prensky M., Digital Natives, Digital Immigrants‘ (2001) 9 On the Horizon 5,1

16. Siemkowicz P., Przestępstwa o charakterze pedofilskim i przeciwko wolności seksualnej popełniane poprzez Internet, w ujęciu polskiego kodeksu karnego, e-Czasopismo Prawa Karnego i Nauk Penalnych 2011, nr 7,

17. Stadniczeńko S.L., Ochrona dziecka przed przemocą, okrucieństwem, wyzyskiem, demoralizacją, zaniedbaniem oraz innym złym traktowaniem /w/ Prawa dziecka po przystąpieniu do Unii Europejskiej (red.) M. Potapowicz, M. Krauzowicz, P. Przybylski.

18. Warylewski J., Pornografia w Internecie – wybrane zagadnienia karnoprawne, Prokuratura i Prawo 2002, nr 4.

19. Wróbel W., Przestępstwa przeciwko ochronie informacji, Rzeczpospolita, nr 206 z 03.09.1993 r.

20. Wróbel W., Uwagi wprowadzające do Rozdziału XXXIII Kodeksu Karnego „Przestępstwa przeciwko ochronie informacji”, w G. Bogdan, K. Buchała, Z. Ćwiąkalski, M. Dąbrowska-Kardas.

Źródła prawa

1. Konstytucja RP z dnia 2 kwietnia 1997, Dz. U. z 1997 r. Nr 78, poz. 483, z późn. zm.

2. Kodeks karny z dnia 6 czerwca 1997 r., Dz. U. z 1997 r. Nr 88, poz. 553 z późn. zm.

3. Kodeks wykroczeń z dnia 20 maja 1971r., t.j. Dz. U. z 2015 r. poz. 1094, z późn. zm.

4. Kodeks cywilny z dnia 23 kwietnia 1964 r. t.j. Dz. U. z 2016 r. Poz. 380 z późn. zm.

5. Ustawa a z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, t.j. Dz. U. z 2015 r. Poz. 2135 z późn. zm.

6. Ustawy z 16 lipca 2004 roku – Prawo telekomunikacyjne, tj. Dz. U. z 2014 r. poz. 243

7. Ustawa z dnia 5 listopada 2009 r. o zmianie ustawy – Kodeks karny, ustawy – Kodeks postępowania karnego, ustawy – Kodeks karny wykonawczy, ustawy – Kodeks karny skarbowy oraz niektórych innych ustaw, Dz.U. Nr 206, poz. 1589

8. Rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 keitnia 2016 roku w sprawie ochrony danych osobowych osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych uchylające dyrektywę 95/46/WE (ogólne rozporządzenie o ochronie danych) 2016 Dz.U.L.119/1

9. Sprawa American Libraries Association v. Pataki (1997) 969 F. Supp.160