14. Cyberzagrożenia a bezpieczne zachowania w Internecie

Sylwester Bębas
ORCID 0000-0002-0659-0895

DOI 10.26399/978-83-66723-65-8/14/s.bebas

Wstęp

Problemy bezpieczeństwa zawsze były integralną częścią życia człowieka, dla którego niezwykle ważne jest poczucie spokoju oraz swobody w dążeniu do realizacji planów[1], i to w każdej dziedzinie życia. Niestety w ostatnim czasie pojęcie bezpieczeństwa nabrało zupełnie nowego znaczenia[2].

Internet niewątpliwie jest narzędziem informacyjno-komunikacyjnym i stanowi platformę wymiany informacji, myśli i doświadczeń. Wyrównuje szanse edukacyjne, daje nieograniczony dostęp do informacji. Od początku swojego istnienia postrzegany jest jako ogromna baza wiedzy, służąc ponadto do rozrywki (np. gry, robienie zakupów), komunikacji, zawierania i podtrzymywania znajomości i bliskich związków, do budowania różnorodnych i wielokierunkowych relacji o charakterze ekonomicznym, politycznym, kulturowym czy społecznym i wielu innych. Człowiek odgrywa w nim rolę zarówno aktywnego odbiorcy, jak

---

[1] Por. E. Jasiuk, A. Szarpak, R. Zielinski, M. Madziala, *Organization of technical rescue operations in the national rescue system*, „Disaster and Emergency Medicine Journal" 2019, t. 4, nr 2, s. 63–67; E. Jasiuk, A. Marchwińska, *Terroryzm lotniczy a ochrona praw jednostki zagwarantowana w Europejskiej konwencji praw człowieka* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa transportu lotniczego*, Warszawa 2021; E. Jasiuk, R. Wosiek, *Global security and safety management in Civil Aviation in light of Annnex 19 to the Chicago Convention* [w:] E. Jasiuk, R. Wosiek (red.), *Legal conditions of international cooperation for the safety and efficiency of civil aviation*, Warszawa 2019, s. 129–140; E. Jasiuk, A. Konert, A. Detyniecka, E. Targońska, *The responsibility of a State in the shooting down of Malaysian Airlines flight MH17*, „Transportation Research Procedia" 2019, t. 43, s. 113–118; A. Chochowska, K. Chochowski, *Bezpieczeństwo lotnictwa cywilnego wobec zagrożenia terroryzmem* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa transportu lotniczego*, Warszawa 2021.

[2] Por. О. Юхимюк, *Особливості викладу принципів права у національному законодавстві. Науковий вісник Херсонського державного університету. Серія: Юридичні науки. Випуск* 6, t. 1, Херсон 2013, s. 12–15; О.М. Юхимюк, *Сумління (сумлінність) судді в міжнародному та національному праві*, „Експерт: парадигми юридичних наук і державного управління" 2021, nr 5(17), s. 57–66; Y. Hofman, A. Demchuk, *Kwestie bezpieczeństwa transportu lotniczego w ustawodawstwie Ukrainy* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa*, *op. cit*.

i aktywnego nadawcy. Internet ma ogromny wpływ na wszystkie przejawy funkcjonowania społeczeństwa.

Obecnie „istnieje potrzeba kreowania choćby powierzchownej więzi społecznej w Internecie np. na portalach społecznościowych lub zaznaczanie swojej obecności poprzez codzienne komentarze na czatach"[3]. Obok ogromnych korzyści, jakie daje szeroko rozumiana cyberprzestrzeń, dochodzi w niej do licznych zachowań antyspołecznych. W przestrzeni sieciowej możemy spotkać się z różnego rodzaju zagrożeniami szczególnie niebezpiecznymi dla dzieci i młodzieży, takimi jak: uzależnienie od Internetu[4], kontakty z przedstawicielami niebezpiecznych środowisk społecznych, uwodzenie dzieci online (*grooming*)[5], cyberpedofilia, cyberpornografia[6], cyberprostytucja dziecięca, cyberseks[7], kontakt z niebezpiecznymi treściami i materiałami mogącymi mieć szkodliwy wpływ na rozwój i psychikę dziecka, utrata prywatności, niewłaściwe udostępnianie informacji, przesyłanie swoich nagich lub półnagich zdjęć (*sexting*), cyberprzestępczość[8], agresja elektroniczna i wiele innych. Dlatego obecnie szczególnie mocno podkreśla się kwestie bezpieczeństwa w Internecie[9].

Żyjemy w świecie, w którym „ludzie powszechnie korzystają z Internetu. I nic w tym dziwnego, bowiem Internet służy do różnych celów do pracy, nauki, rozrywki, komunikacji itp. Używany jest przez osoby w różnym wieku, z różnym wykształceniem. Oprócz zalet niesie ze sobą wiele zagrożeń. Codziennie wykradanych jest wiele miliony rekordów, pojawia się też wiele prób złośliwego oprogramowania. Dane użytkowników sieci stały się cennym towarem na

[3] T. Szlendak, *Wielozmysłowa kultura iwentu. Skąd się wzięła, czym się objawia i jak w jej ramach oceniać dobro kultur*, „Kultura Współczesna. Teoria. Interpretacje. Praktyka" 2010, nr 4(66), s. 93.

[4] Por. S. Bębas, *Uzależnienie od komputera, Internetu* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica,* Toruń 2014, s. 194–196.

[5] Por. S. Bębas, *Uwodzenie dzieci przez Internet* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy...*, *op. cit.*, s. 190–191.

[6] Por. S. Bębas, E. Jasiuk, *Pedofilia i pornografia w Internecie – wybrane aspekty pedagogiczne i prawnomiędzynarodowe* [w:] J. Bukała, K. Wątorek (red.), *Stop pedofilii*, Kielce 2012, s. 89–111; *idem*, *Krzywdzenie dziecka w sieci – wybrane aspekty profilaktyki* [w:] J. Bukała, K. Wątorek (red.), *Krzywdzenie dziecka – zapobieganie przemocy*, Kielce 2013, s. 45–64.

[7] Por. S. Bębas, *Cyberseks* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy...*, *op. cit.*, s. 45–46.

[8] Por. S. Bębas, *Cyberprzestępczość* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy...*, *op. cit.*, s. 40–42.

[9] Por. S. Bębas, T. Konopka, *Selected aspects of security and risks in cyberspace* [w:] G. Sobolewski, A. Cyran (red.), *The practical and theoretical approach to the issue of security*, Kielce 2013, s. 69–80; *idem*, *Patologie i zagrożenia w świecie wirtualnym* [w:] S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberświecie*, Radom 2012, s. 329–345; *idem*, *Bezpieczeństwo w cyberświecie* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy...*, *op. cit.*, s. 22–24.

rynku cyberprzestępczym. Zakupem takich informacji zainteresowani są także tzw. brokerzy danych. Skupują oni informacje o ludziach, aby później sprzedać je zainteresowanym firmom"[10].

Celem niniejszego opracowania jest analiza wybranych obszarów w badaniach nad bezpieczeństwem i zagrożeniami w sieci. Problem badawczy zawiera się w pytaniu: jak powinna wyglądać skuteczna edukacja i profilaktyka dla bezpieczeństwa dzieci i młodzieży w Internecie? Zamiarem badawczym jest ukazanie podejmowanej tematyki w perspektywie integralnego, szeroko rozumianego wychowania ukierunkowanego na mądre, racjonalne, konstruktywne i bezpieczne korzystanie z sieci. Zastosowanie metody analizy i syntezy pozwoliło na przedstawienie współczesnych osiągnięć naukowych dotyczących skali zjawiska zagrożeń i patologii w Internecie, zwłaszcza dla dziecka – jej przyczyn, uwarunkowań i konsekwencji. Ujęcie syntetyczne pozwoliło na wyprowadzenie wniosków i podanie sugestii dotyczących wychowania, edukacji i profilaktyki w kontekście zagrożeń medialnych.

Zagrożenia techniczne

„Wirus" to powszechna nazwa szkodliwego, niechcianego oprogramowania, które ktoś siłą instaluje na urządzeniach podpiętych do sieci. Technologiczną „szczepionką" na wirusy są programy antywirusowe. Ważna jest świadomość zagrożenia i schemat bezpiecznych, „higienicznych" zachowań, mogących uchronić przed zainfekowaniem. Wirusy mogą zaatakować nie tylko komputer lub smartfon, ale także inne urządzenia. Najczęściej urządzenia elektroniczne infekowane są wirusami typu:

- *cross-site scripting* – to luka w zabezpieczeniu strony umożliwiająca hakerom umieszczenie szkodliwego skryptu na zaufanej stronie lub w zaufanej aplikacji, który powoduje zainstalowanie złośliwego oprogramowania w przeglądarkach użytkowników;
- koń trojański – to oszustwa i metody inżynierii społecznej, zachęcające do uruchamiania pozornie łagodnych programów komputerowych, które ukrywają jednak złośliwy kod;
- *rootkit* – może on zostać zainstalowany razem z różnymi rodzajami produktów i wykorzystany do zdalnej kontroli urządzenia;

[10] A. Kolek, *Zachowania dyssocjalne młodzieży w przestrzeni internetowej. Implikacje pedagogiczne*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1, s. 50–51.

- *keylogger* – jest to rodzaj oprogramowania szpiegującego, które potajemnie rejestruje naciśnięcia klawiszy, więc złodzieje mogą uzyskać informacje o koncie, kartach kredytowych, nazwach użytkowników, hasłach i innych danych osobowych;
- robaki komputerowe – to zagrożenia, które mogą same się powielać i spowalniać komputer;
- programy szpiegujące typu *spyware*, które są rodzajem oprogramowania, które trudno wykryć, gromadzą informacje na temat zwyczajów, surfowania w Internecie, historii przeglądania lub poufne dane;
- *malware* – wykorzystywane do wykradania danych osobowych, haseł i pieniędzy oraz blokowania dostępu do urządzeń;
- *adware* – to rodzaj wolnego oprogramowania wspieranego przez reklamy; niektóre z tego typu zagrożeń zbierają nasze prywatne informacje, śledzą strony, które odwiedza internauta, a nawet rejestrują sekwencje klawiszy;
- oprogramowanie *ransomware* – ogranicza dostęp do systemu komputerowego i wymaga zapłacenia okupu, aby blokada została usunięta;
- *backdoor* – to luka w zabezpieczeniach systemu utworzona umyślnie w celu późniejszego wykorzystania;
- pacynka – to fałszywe konto utworzone na dowolnej aplikacji umożliwiającej użytkownikowi interakcje z innymi odbiorcami; *fake*-konta są częścią inżynierii społecznej mającej na celu przekazanie lub wyłudzenie określonych informacji bądź nakłonienie do realizacji określonych działań;
- *botnet* – to aplikacja, która wykonuje powtarzalne czynności w sieci.

Bardzo ważne jest, aby prawidłowo chronić urządzenia, z których korzysta internauta: ostrożnie korzystać z publicznego WI-FI, tworzyć silne hasła, uważać na podejrzane wiadomości SMS i e-maile, instalować programy antywirusowe, aktualizować oprogramowanie, sprawdzać wiarygodność aplikacji. Gdy urządzenie zdradza oznaki zainfekowania, należy je odłączyć od Internetu i sieci lokalnej, spróbować uruchomić w trybie awaryjnym i jeśli jest taka możliwość, skopiować swoje dane, zainstalować program antywirusowy, zainstalować oprogramowanie i bazę wirusów najlepiej z poziomu niezainfekowanego komputera oraz wykonać pełne skasowanie systemu.

Zagrożenia dla dzieci i młodzieży

Słowo *sexting* oficjalnie pojawiło się w 2009 roku[11]. Termin „seksting" (ang. *sexting*) „powstał na początku bieżącego stulecia z połączenia słów *sex* oraz *texting* w odniesieniu do zjawiska przesyłania między użytkownikami telefonów komórkowych wiadomości tekstowych o charakterze seksualnym"[12]. Seksting to zjawisko polegające na „przesyłaniu za pośrednictwem sieci lub publikowaniu *online* osobistych materiałów o charakterze erotycznym lub pornograficznym"[13].

Sexting to „wysyłanie roznegliżowanych zdjęć lub krótkich filmików o treści erotycznej do drugiej osoby. Zazwyczaj przesyłanie takich materiałów odbywa się za pomocą telefonu komórkowego (usługa MMS) i Internetu (e-mail). Możemy tu wyróżnić dwa rodzaje zachowań: samoistne wykonanie fotografii lub krótkiego filmiku i dobrowolne wysłanie do osoby, z którą nie wiąże nadawcy relacja seksualna; samoistne wykonanie własnej fotografii lub filmiku (bądź zgoda na wykonanie tej czynności przez osobę zaufaną) i dobrowolne wysłanie bądź przekazanie osobie (chłopakowi, dziewczynie), z którą wiąże nadawcę relacja seksualna"[14].

Niektórzy w definiowaniu uczestników sekstingu „ograniczają ich do dzieci i młodzieży, inni nie stawiają ograniczeń wiekowych. Różnie określa się też charakter obrazów przesyłanych w ramach sekstingu – od ogólnego terminu «materiały o charakterze seksualnym» przez bardziej określone, ale w dalszym ciągu szerokie pojęcie «nagie lub prawie nagie», po definicje ograniczające zjawisko do przesyłania materiałów niezgodnych z prawem, czyli określanych potocznie mianem pornografii dziecięcej"[15]. W zależności od przyjętej definicji i metodologii badań „problem ten dotyczy od kilku do nawet ponad 40% dzieci i nastolatków"[16].

Obecnie „wyróżnia się nowy typ sextingu, angażujący technologię przekazu komunikatów za pomocą kamery internetowej dołączonej do komputera

---

[11] Por. H.K. Hudson, *Factors affecting sexting behaviors among selected undergraduate students*, Charleston 2006, s. 1; B.S. Marker, *Sexting as moral panic. An explanatory study into the media's construction of sexting*, Richmond 2009, s. 1–46.

[12] D. Siegle, *Cyberbullying and sexting: technology abuses of the 21st century*, „Gifted Child Today" 2010, t. 32, nr 2, s. 14–16.

[13] K.J. Mitchell, D. Finkelhor, L.M. Jones, J. Wolak, *Prevalence and characteristics of youth sexting. A national study*, „Pediatrics" 2012, nr 129(1), s. 13–20.

[14] Por. W. Ronatowicz, *Ryzykowne zachowania seksualne dzieci, młodzieży i młodych dorosłych w kontekście korzystania z technologii cyfrowych*, „Rocznik Lubelski" 2014, t. 40, cz. 1, s. 129–143.

[15] K. Lounsbury, K.J. Mitchell, D. Finkelhor, *The true prevalence of „sexting". Crimes against children research centre*, 2011 [online:] https://scholars.unh.edu/cgi/viewcontent.cgi?article=1063&context=ccrc [dostęp: 20.08.2023].

[16] Ł. Wojtasik, *Seksting wśród dzieci i młodzieży*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, nr 13(2), s. 89–91.

bądź zainstalowanej w komputerze przenośnym (laptop) w czasie rzeczywistym (*online*). To rodzaj sextingu przy użyciu wideoczatów, czyli portali, gdzie oprócz tradycyjnej pisemnej formy komunikacji użytkownicy mogą komunikować się ze sobą za pomocą mikrofonu oraz kamery internetowej w czasie realnym i w ten sposób prezentować zachowania seksualne. Najbardziej popularnymi zachowaniami są striptiz, masturbacja, petting i stosunek seksualny"[17].

Sexting jest obecnie „powszechną praktyką w grupach nastolatków, służącą najczęściej flirtowaniu, okazywaniu miłości, przywiązania i zaufania, ale również nawiązywaniu relacji o charakterze seksualnym. W przypadkach skrajnych może służyć do prześladowania i upokarzania tych, którzy zdecydowali się wziąć w niej udział, szczególnie poprzez rozpowszechnienie zdjęć wśród znajomych, wgrywanie ich do Internetu, czy w inny sposób udostępnienie szerokiemu gronu odbiorców. Takie działania mogą prowadzić w konsekwencji do cyberbullyingu, który pojawia się, gdy jedna osoba lub grupa podejmują działania mające na celu zastraszenie, poniżenie, skrzywdzenie jednostki biorącej udział w procederze sextingu przy użyciu materiałów przez nią często dobrowolnie udostępnionych"[18].

Anonimowość i eksterytorialność „związana z korzystaniem z Internetu sprzyja aktom nadużyć seksualnych, popełnianych na szkodę dzieci i młodzieży, w tym szeroko pojmowanym aktom przemocy seksualnej w postaci pedofilii"[19].

Pedofilia to według Z. Lwa-Starowicza „popęd, psychoseksualna skłonność do dzieci, młodzieży, która może wynikać z pewnych zmian w mózgu, jak i z uwarunkowań psychicznych wynikających m.in. z przemocy seksualnej w dzieciństwie"[20]. J. Warylewski wskazuje, że „pedofilia jest określeniem, które ma wiele różnorodnych desygnatów"[21].

---

[17] Użytkownicy wideoczatów bardzo często decydując się na podjęcie zachowań seksualnych, starają się chronić swój prywatny wizerunek poprzez zakładanie masek, okularów przeciwsłonecznych bądź kadrując kamerę w ten sposób, aby twarze „bohaterów" były niewidoczne. Niestety, wielokrotnie użytkownicy w trakcie wzrostu podniecenia seksualnego tracą czujność, pokazując swoje twarze, mówiąc do swoich partnerów po imieniu. Użytkownicy takich serwisów często nieuważnie dobierają miejsce nagrywania swoich zachowań seksualnych. Do niefrasobliwych zachowań możemy zaliczyć: nieusunięcie z drugiego planu swoich realnych zdjęć, dyplomów uznania z imieniem i nazwiskiem. W. Ronatowicz, *Ryzykowne zachowania...*, *op. cit.*, s. 129–143.

[18] J. Lopez, *Has the Internet unleashed digital drama?*, „Momentum" 2011, vol. 42, nr 4, s. 20–23.

[19] A. Kubala-Kulpińska, *Seksting czyli wirtualny ekshibicjonizm, który może śledzić cały świat*, „Głos Pedagogiczny" 2015, nr 68, s. 44–46.

[20] Z. Lew-Starowicz, *Seks w sieci i nie tylko*, Kraków 2003, s. 207.

[21] Wyróżnia się: nepidofilię – popęd skierowany do dzieci w wieku przedszkolnym, pedofilię właściwą – popęd do dzieci w wieku szkolnym, przed okresem dojrzewania, i efebofilię oraz hebefilię – skierowanie popędu do osób w wieku dojrzewania. Nie każdy jednak czyn pedofilny jest popełniany przez pedofila. Dla większości sprawców przestępstw seksualnych małoletni jest

Wykorzystywanie seksualne dziecka rozumiane jako „włączanie dziecka w aktywność seksualną z dorosłym jest powszechnie oceniane negatywnie, co znajduje swój wyraz zarówno w treści norm obyczajowych, jak i prawnych niemal wszystkich kultur i krajów świata. Przejawy seksualności u dzieci są wprawdzie prawidłowością rozwojową, ale w żadnej mierze nie usprawiedliwiają relacji seksualnej osoby dorosłej z dzieckiem. Nigdy bowiem nie jest to relacja symetryczna w wymiarze rozumienia istoty takich zachowań i świadomego decydowania o nich – dorosły zawsze ma przewagę nad dzieckiem"[22].

Spektrum „bezpośrednich i długofalowych skutków wykorzystywania seksualnego dziecka jest szerokie, a ich wystąpienie w dużej mierze zależy od etapu rozwojowego dziecka w momencie wykorzystania, osoby sprawcy, drastyczności i czasu trwania wykorzystywania oraz od tego, czy ujawniło swoje doświadczenia i czy dostało wsparcie od najbliższych"[23].

Grooming oznacza szczególną relację między dziećmi (nastolatkami) a osobami dorosłymi polegającą na uwodzeniu dzieci w Internecie przez dorosłych w celu wykorzystania seksualnego[24]. Poprzez *grooming* potocznie rozumie się uwodzenie dzieci przez Internet. Pojęcie to pochodzi z języka angielskiego i w sensie dosłownym oznacza „pielęgnowanie i opiekowanie, jakie pedofil roztacza nad swoją potencjalną nieletnią ofiarą"[25].

Poprzez „nieustanny kontakt z ofiarą za pomocą środków komunikacji elektronicznej sprawca doprowadza zwykle do spotkania w świecie realnym bądź do pozyskania interesujących go materiałów, np. o charakterze pornograficznym. Zdarza się również, że sprawca skraca czas poświęcony na uwodzenie dziecka, przechodząc do etapu, w którym jest możliwe użycie przez niego przemocy, np. zmuszenia dziecka do poddania się czynnościom seksualnym w trakcie zainicjowanego spotkania"[26].

Wraz ze wzrostem swojej popularności Internet stał się kolejną płaszczyzną, na której rozkwita ludzka seksualność. Oprócz dystrybucji pornografii umożliwia

często „obiektem zastępczym", „sytuacyjnym" lub „okazjonalnym". J. Warylewski, *Reakcja karna na przestępstwa seksualne*, „Przegląd Więziennictwa Polskiego" 2007, nr 54, s. 43.

[22] M. Skierkowska, *Edukacyjne programy profilaktyki wykorzystania seksualnego dzieci*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, nr 13(1), s. 142.

[23] M. Beisert, A. Izdebska, *Wykorzystanie seksualne dzieci*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2012, nr 39(2), s. 64–66.

[24] K. Fenik, *Grooming. Uwodzenie dzieci w Internecie* [w:] A. Jodko (red.), *Tabu seksuologii*, Warszawa 2008, s. 136.

[25] K. Banasik, *Głos w dyskusji o art. 200a k.k.*, „Palestra" 2010, nr 3.

[26] Por. M. Wojtas, *Proces uwodzenia dzieci w Internecie* [w:] *Dziecko w sieci. Zapobieganie wykorzystywaniu seksualnemu dzieci w Internecie. Profilaktyka, Prewencja. Nowa legislacja*, Warszawa 2010, s. 7–8.

on także kontaktowanie się ludzi, którzy chcieliby zaspokajać swoje potrzeby seksualne w sieci[27].

Pod pojęciem cyberseksu najczęściej rozumie się „komunikację synchroniczną prowadzoną wirtualnie zazwyczaj przez dwie osoby, które wymieniają się komunikatami poświęconymi swoim fantazjom seksualnym, czemu towarzyszy masturbacja jednej lub obydwu stron; w tym celu osoby te używają do tego specjalnych kamer; cyberseks może uzależniać, dlatego zawiera w sobie element autodestrukcji"[28].

Cyberseks jest interakcją co najmniej dwóch osób związaną z używaniem materiałów elektronicznych (tekstu, obrazu, dźwięku) za pośrednictwem Internetu w celu stymulacji lub osiągnięcia pobudzenia seksualnego. Najczęściej przybiera on jednak formę pisemną i jest to komunikacja synchroniczna za pomocą Internetu, czyli spotkanie na czacie, nierzadko ubarwione obrazem z kamery, jeśli czat daje taką możliwość. Czaty takie są ogólnodostępne, portale o tematyce erotycznej funkcjonują przy każdej z większych polskich przeglądarek i większość z nich ma również możliwość przekazywania i odbierania obrazu z kamery. Komunikaty pisemne mogą przyjmować formę dosłownych opisów czynności seksualnych lub rozbudowanej fabuły obejmującej opis całego otoczenia i ról odgrywanych przez komunikujące się osoby. Czasem bywanie na czacie prowadzi także do jakiejś innej formy zaspokajania popędu, na przykład do skatologii telefonicznej (prowadzenia obscenicznych rozmów przez telefon z osobami poznanymi na czacie)[29].

---

[27] Por. M. Dąbrowska, *Grooming: wybrane aspekty prawnokarne i kryminologiczne*, Warszawa 2018; A. Przedlacka, *Seksualność w Internecie – zagrożenia i korzyści dla rozwoju psychoseksualnego dzieci i młodzieży*, „Meritum" 2019, nr 3, s. 25–31; J.R. Temple, A.P. Jonathan, P. Van Den Berg, V.D. Le, A. McElhany, B.W. Temple, *Teen sexting and its association with sexual behaviors*, „The Archives of Pediatrics & Adolescent Medicine" 2012, nr 166(9), s. 828–833; K.R. Taylor, *„Sexting": fun or felony?*, „Principal Leadership" 2009, vol. 9, nr 8, s. 60–62; D. Corbett, *Let's talk about sext. The challenge of finding the right legal response to the teenage practice of 'sexting'*, „Journal of Internet Law" 2009, nr 12, s. 3–8; F.C. Heynemann, *Seksting i grooming*, „Dyrektor Szkoły" 2015, nr 6, s. 74–77.

[28] Por. M.T. Witty, A.N. Carr, *Wszystko o romansie w sieci. Psychologia związków internetowych*, przekł. T. Kościuczuk, Gdańsk 2009, s. 140.

[29] Por. A. Leśnicka, *Cyberseks w polskim Internecie – ankieta dla użytkowników czatów erotycznych,* „Seksuologia Polska" 2009, nr 7, 1, s. 9–14; J. Chmielecka, *Internet złych rzeczy*, Bielsko-Biała 2017; S. Polcyn-Matuszewska, *Cyberzagrożenia dla dzieci i młodzieży*, „Remedium" 2017, nr 9, s. 28–29; A. Kałuba-Korczak, *Dziecko w internecie – zagrożenia*, „Wychowanie w Przedszkolu" 2017, nr 5, s. 14–17; S. Pawłowska, *iGen – pokolenie Internetu*, „Remedium" 2019, nr 12, s. 22–24; A. Ben-Ze'ev, *Miłość w sieci. Internet i emocje*, przekł. A. Zdziemborska, Poznań 2005, s. 247.

Pojęcie pornografii „wywodzi się z języka greckiego: *pórne* – nierządnica; *gráphein* – skrobać, rytować, rysować, pisać; *pornográphos* – piszący o nierządnicach”[30]. Pornografia „nie jest terminem zdefiniowanym ustawowo. W próbach wyjaśnienia tego pojęcia można dostrzec dwie zasadnicze grupy poglądów”[31]. Od lat trwają batalie o zdefiniowanie i uściślenie słowa „pornografia”. „Problem polega na tym, że to, co dla jednych jest pornografią, dla innych może być erotyką bądź zachowaniem obscenicznym. Rozumienie tego pojęcia zmienia się w zależności od czasu i ma tyle znaczeń, ile krajów, umysłowości, obyczajów i systemów kulturowych”[32].

Termin „cyberpornografia” zawiera w swoim znaczeniu nowe aspekty:

- „komercjalizacja i normalizacja aktów/zachowań stygmatyzowanych na rynkach tradycyjnych (to drugie sprowadziło pornografię do podziemia);
- pojawienie się zjawiska związanego z wyzwolonym wyrażaniem samego siebie oraz grupowym uprawomocnieniem (co można określić jako wzrost ekspresyjnej seksualności);
- nowy związek między producentem i konsumentem, w którym na podstawie informacji zwrotnej (zwanej «czego chcą konsumenci») rozwijane są nowe techniki i prezentowane treści;
- redefinicja pornografii samej w sobie jako formy rozrywki, funkcji edukacyjnej i stylu życia”[33].

Cyberprzemoc „to rodzaj przemocy w sieci. Prześladowca straszy, poniża, obraża ofiarę poprzez komentarze w mediach społecznościowych, czy robienie jej zdjęć lub kręcenie filmów bez jej zgody. Następnie materiały umieszcza na ogólnodostępnych witrynach odwiedzanych przez wiele osób. Napastnicy często prześladują i utrudniają życie swoim ofiarom również wysyłając im obraźliwe SMS-y lub e-maile”[34].

---

[30] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Warszawa 1999, s. 399.

[31] Poglądy opierające się na ujęciu subiektywistyczno-moralistycznym oraz obiektywistyczno-pragmatycznym. Pierwszy głosi, że pornograficzna treść to taka, która według zamiaru sprawcy ma służyć wyłącznie lub przede wszystkim wywołaniu podniecenia seksualnego u odbiorcy przekazu, natomiast według drugiego – decydujące jest nie nastawienie sprawcy, ale obiektywna treść prezentacji i jej intersubiektywny społeczny odbiór – zob. M. Filar, *Pornografia. Studium z dziedziny polityki kryminalnej*, Toruń 1977, s. 30–57.

[32] Por. A. Krawulska-Ptaszyńska, *Psychospołeczne uwarunkowania korzystania z pornografii przez mężczyzn*, Poznań 2003, s. 10.

[33] B. Cronin, E. Davenport, E. Zones, *Positioning pornography in the digital economy*, „The Information Society” 2001, nr 17(1), s. 33–48.

[34] Por. J. Pyżalski, *Bezpieczny Internet w szkole – jak zapobiegać cyberprzemocy?* „Głos Pedagogiczny” 2018, nr 97, s. 16–19.

W szerokim ujęciu „agresję elektroniczną definiować możemy jako wszystkie intencjonalne akty (nastawione na zadanie bólu, krzywdy czy zniszczenie jakichś dóbr), które realizowane są za pomocą nowych mediów. W opisie zjawiska badacze zwracają uwagę na stosowanie różnego rodzaju nowoczesnych technologii (głównie komunikacyjnych) w celu krzywdzenia innej osoby"[35]. *Cyberbullying* stanowi szczególną formę mobbingu[36]. Literatura przedmiotu zawiera liczne definicje tego zjawiska[37]. Jest to problem, z którym borykają się kraje na całym świecie. Podjęcie tego tematu to niezwykle ważne zadanie, bowiem jest to problem jeszcze mało poznany, nieczęsto dyskutowany w polskiej literaturze przedmiotu, jak również rzadko podejmowany w badaniach naukowych[38]. Bardzo cenny wydaje się w rozpoznaniu tego problemu w Polsce dorobek J. Pyżalksiego[39].

---

[35] Por. J. Pyżalski, *Gimnazjaliści online: dobre i złe wiadomości z polskiej części wyników European Cyberbullying Intervention Project* [w:] J. Pyżalski (red.), *Cyberbullying. Zjawisko, konteksty, przeciwdziałanie*, Łódź 2012, s. 18.

[36] Por. R. Kowalski, S. Limber, *Electronic Bullying Among Middle School Students*, „Journal of Adolescent Health" 2007, nr 41, s. 22–30; J. Pyżalski, *Cyberbullying – stare wino w nowej butelce?* [w:] L. Jakubowska-Malicka, A. Kobylarek, M, Pryszmont-Ciesielska (red.), *Audiowizualność. Cyberprzestrzeń. Hipertekstualność. Ponowoczesne konteksty edukacji*, Wrocław 2009, s. 183; B. Białecka, *Jak radzić sobie z cyberprzemocą?,* „Wychowawca" 2019, nr 11, s. 30–31; A. Gregorek, *Mindfulness – trening uważności dzieci i młodzieży w profilaktyce cyberprzemocy*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1, s. 30–38.

[37] *Cyberbullying* ma miejsce, jeśli ktoś powtarzalnie naśmiewa się z innej osoby w sieci lub nęka ją poprzez e-maile lub wiadomości tekstowe lub gdy zamieszcza coś w Internecie o osobie, której nie lubi. Por. S. Hinduja, J.W. Patchin, *Cyberbullying: Neither an epidemic nor a rarity*, „European Journal of Developmental Psychology" 2012, nr 9(5), s. 539–543. *Cyberbullying* to agresywny, zamierzony akt dokonany przez grupę lub jednostkę przy użyciu elektronicznych form komunikacji, w sposób powtarzalny, przed którym ofiara nie może się łatwo bronić. Por. P.K. Smith, J. Mahdavi, M. Carvalho, S. Fisher, S. Russell, N. Tippett, *Cyberbullying: its nature and impact in secondary school pupils*, „Journal of Child Psychology and Psychiatry" 2008, nr 49(4), s. 376; Z. Małysz, *Agresywność, agresja, przemoc, bullying i cyberbullying jako problemy opiekuńczo-wychowawcze XXI wieku*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1, s. 12–20.

[38] Por. S. Bębas, *Cyberprzemoc jako przejaw współczesnej patologii społecznej w świecie wirtualnym* [w:] K. Marzec-Holka, K. Mirosław-Nawrocka, J. Moleda (red.), *Współczesne uwarunkowania i wzory procesów resocjalizacji, reintegracji, inkluzji,* Warszawa 2014, s. 557–575; *idem*, *Cyberstalking – wybrane problemy prawne i pedagogiczne* [w:] R. Frey (red.), *Przemiany prawa publicznego i prywatnego na początku XXI wieku*, Kielce 2012, s. 35–49; *idem*, *Cyberprzemoc* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014, s. 38–39; *idem*, *Cyberprześladowanie* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014, s. 43–44; *idem*, *Patologie społeczne w sieci*, Toruń 2013, s. 49–74.

[39] J. Pyżalski, *Agresja elektroniczna – wirtualne ciosy, realne rany – cz. I*, „Remedium" 2008, nr 186(9), s. 26–27; *idem*, *Agresja elektroniczna – wirtualne ciosy, realne rany – cz. II*, „Remedium"

Klasyczne formy cyberbullyingu to:

- „prześladowanie – może być definiowane jako powtarzające się wysyłanie obraźliwych wiadomości lub pogróżek innym osobom za pośrednictwem wiadomości e-mail, SMS, komunikatora, w *chat roomach*;
- oczernianie – to rozsyłanie plotek za pomocą urządzeń komunikacji elektronicznej; w przeciwieństwie do plotkowania w życiu prawdziwym, informacja w Internecie może zostać rozesłana do tysięcy ludzi w ciągu kilku sekund;
- ujawnianie – ma miejsce, gdy ujawnione zostaną informacje prywatne, które ofiara wysłała komuś w zaufaniu; wówczas są one przesyłane dalej w celu skompromitowania ofiary;
- wykluczenie – jest odpowiednikiem wykluczenia w prawdziwym życiu i oznacza brak możliwości uczestniczenia w życiu społecznym; w kontekście wirtualnego świata może to oznaczać wykluczenie z gier, czatów, platform”[40].

Ponadto w literaturze przedmiotu wyróżnia się kilka odmian, w jakich przejawia się cyberprzemoc:

- „flaming – wysyłanie agresywnych, wulgarnych wiadomości o konkretnej osobie do grupy lub do niej samej przez e-mail lub inną formę komunikacji tekstowej;
- zastraszanie *online* – powtarzalne wysyłanie obraźliwych wiadomości e-mailowych lub w innej formie tekstowej do osoby zastraszanej;
- cyberstalking – zastraszanie *online* w formie pogróżek;

2008, nr 186(10), s. 28–29; *idem*, *Agresja elektroniczna dzieci i młodzieży. Różne wymiary zjawiska*, „Dziecko Krzywdzone” 2009, nr 1(26), s. 12–27; *idem*, *Agresja elektroniczna i mobbing elektroniczny w kontekście zaangażowania w stosowanie nowych technologii komunikacyjnych*, „Kwartalnik Pedagogiczny” 2009, nr 4, s. 31–52; *idem*, *Cyberbullying – stare wino w nowej butelce* [w:] L. Jakubowska-Malicka, A. Kobylarek, M. Pryszmont-Ciesielska (red.), *Audiowizualność. Cyberprzestrzeń. Hipertekstualność. Ponowoczesne konteksty. Edukacja*, Wrocław 2009; *idem*, *Agresja elektroniczna wśród 15-latków w Polsce* [w:] K. Okulicz-Kozaryn, K. Ostaszewski (red.), *Promocja zdrowia psychicznego. Badania i działania w Polsce*, Warszawa 2010; *idem*, *Agresja w materiałach publikowanych w Internecie przez użytkowników – flirt tradycyjnych i nowych mediów* [w:] J. Drozdowicz, M. Bernasiewicz (red.), *Kultura popularna w społeczeństwie współczesnym. Teoria i rzeczywistość*, Kraków 2010; *idem*, *Agresja rówieśnicza online i offline wśród gimnazjalistów. Wybrane uwarunkowania i konsekwencje* [w:] B. Szmigielska (red.), *Edukacja w dwóch światach offline i online*, Kraków 2011.

[40] V. Lubkina, G. Marzano, *Zapobieganie cyberprzemocy* [w:] J. Lizut (red.), *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Warszawa 2014, s. 111.

- dyskredytacja – wysyłanie nieprawdziwych, oszczerczych, okrutnych informacji o określonej osobie do innych lub zamieszczanie takich informacji *online*;
- podszywanie się pod kogoś – podszywanie się pod konkretną osobę i wysyłanie lub zamieszczanie informacji w jej imieniu w sieci w celu poniżenia jej;
- wykluczenie – wykluczenie w okrutny sposób kogoś z grupy *online*"[41].

J. Pyżalski wskazał na następujące rodzaje agresji elektronicznej:

- „agresja elektroniczna wobec pokrzywdzonych, czyli osób «słabszych od sprawcy»;
- agresja elektroniczna wobec celebrytów, czyli osób znanych, pojawiających się w mediach;
- elektroniczna agresja uprzedzeniowa wobec określonej grupy ludzi, np. konkretnej narodowości;
- agresja elektroniczna wobec nieznajomych, czyli wybranych przypadkiem;
- mobbing elektroniczny stosowany wobec osób z tej samej grupy, do której należy sprawca"[42].

Bardzo często „sprawcami agresji w Internecie są osoby o niskich kompetencjach społecznych, nie potrafiące nawiązać komunikatywnego kontaktu z drugim człowiekiem. Konsekwencje stosowania cyberprzemocy są poważne, często objawiają się jako niskie poczucie własnej wartości, lęki, koszmary senne, bóle głowy i brzucha oraz trudności z zasypianiem. Osoby pokrzywdzone stają się zalęknione i odczuwają silne poczucie winy za zaistniałą sytuację (…). [Cyberprzemoc – przyp. aut.] w skrajnych przypadkach prowadzi do chorób psychicznych"[43].

Podsumowanie

Korzystając z Internetu, „nie powinno się używać tego samego loginu i hasła do wielu usług i serwisów. Należy myśleć o tym, komu i w jakim celu udostępnia się dane. Nie każdy serwis musi wiedzieć wszystko o jego użytkowniku. Jeżeli jest taka możliwość, zawsze powinno się korzystać z uwierzytelniania dwuetapowego, np. potwierdzenia logowania kodem SMS, odciskiem palca, czy korzystać z systemu rozpoznawania twarzy. Należy chronić dane wrażliwe, m.in.: imię

[41] N.E. Willard, *Cyberbullying and cyberthreats. Responding to the challenge of online social aggression, threats, and distress*, San Francisco 2007.

[42] J. Pyżalski, *Agresja elektroniczna wśród dzieci i młodzieży*, Sopot 2011, s. 42.

[43] M. Krajewska, *Cyberprzemoc w kontaktach rówieśniczych*, „Opieka, Wychowanie, Terapia" 2010, nr 1/2, s. 12–19.

i nazwisko, numer identyfikacyjny (np. PESEL, NIP, numer dowodu osobistego), adres zamieszkania, adres mailowy, data urodzin, płeć, kolor oczu, wagę, wzrost, dane ujawniające pochodzenie rasowe lub etniczne, dane ujawniające poglądy polityczne, dane ujawniające przynależność do związków zawodowych, dane genetyczne, dane biometryczne, czy dane dotyczące zdrowia. Nie należy udostępniać też innych informacji, dotyczących np. numerów telefonów, kont czy kart kredytowych"[44].

Należy „być ostrożnym z publikowaniem zdjęć. Nie powinno się publikować w sieci zdjęć, na których ktoś jest niekompletnie ubrany, zdjęć wnętrz mieszkań, zdjęć drogich przedmiotów, zdjęć z wakacji, czy zdjęć z prywatnych spotkań. Korzystając z sieci, należy czytać regulaminy. Dość często ludzie sami wyrażają zgodę na to, aby ich dane, które przesyłają w jakieś miejsce w sieci lub udostępniają określonej aplikacji lub serwisowi internetowemu, były udostępniane lub odsprzedawane innym osobom lub firmom. Informacje o tym znajdują się właśnie w regulaminach. Za każdym razem, gdy ktoś instaluje nową aplikację na telefonie lub tablecie, rejestruje się do nowego serwisu czy usługi, powinien uważnie przeczytać regulamin i zastanowić się, na co właściwie się zgadza"[45].

Korzystając z sieci, należy „tworzyć bezpieczne hasła. W dzisiejszym świecie Internetu haseł używamy w zasadzie bez przerwy, przy logowaniu do poczty elektronicznej, bankowości *online*, dokonując zakupów lub uzyskując dostęp do rozmaitych urządzeń itp. Użytkownicy Internetu, aby łatwiej zapamiętać hasła, używają haseł krótkich, łatwo kojarzących się np. z imieniem swoich zwierząt, bohaterów z filmów, z datą swoich urodzin itp. Takie hasło niestety może być złamane w kilka sekund. Tymczasem silne hasło nie powinno być słownikowym wyrazem, ale powinno zawierać długi ciąg dużych i małych liter, cyfr i znaków specjalnych"[46].

Bardzo dobrym rozwiązaniem „podczas korzystania z Internetu jest tzw. uwierzytelnianie wielopoziomowe, czyli sposób zabezpieczenia oraz autoryzacji podczas logowania przed skorzystaniem z konta użytkownika przez niepowołane osoby poprzez zdobycie przez nią identyfikatora użytkownika i hasła uwierzytelniającego. Oprócz podania tych danych logowania, użytkownik musi: podać uzyskany kod lub frazę np. ze swojego przenośnego urządzenia internetowego, poprzez przepisanie go z e-maila wysłanego przez serwis, na którym

[44] B. Białecka, *Niebezpieczne zachowania w Internecie*, „Wychowawca" 2019, nr 9, s. 14–15.

[45] M.M. Jankowska, *Psychoedukacja rodziców na temat cyberprzemocy*, „Głos Pedagogiczny" 2020, nr 115, s. 28–33.

[46] I. Gołębiewska, *Cyberprzemoc – zagrożenie dla młodego pokolenia*, „Wychowawca" 2010, nr 7/8, s. 12–15; Ł. Wojtasik, *Cyberprzemoc*, „Remedium" 2008, nr 2, s. 4–5.

użytkownik próbuje się zalogować, czy też za pomocą specjalnej karty, linii papilarnych palca"[47].

Bardzo ważne jest, „aby stosować zasady bezpieczeństwa podczas komunikowania się przez Internet. Nie powinno się rozmawiać z nieznajomymi, poza przypadkami uzasadnionymi, np. sprzedawcą w sklepie internetowym, lekarzem. Wszystkie osoby, z którymi nawiązywany jest kontakt w sieci, nie powinny być anonimowe, tzn. nieznane z imienia i nazwiska. W żadnym wypadku nie powinno się wysyłać nieznajomym plików, w tym zdjęć i filmów, przesyłać spamu, w tym tzw. łańcuszków szczęścia, czy otwierać wiadomości z podejrzanymi linkami, które mogą zawierać wirusy i posłużyć do okradzenia danej osoby"[48].

Niezwykle istotne jest to, aby korzystając z Internetu, „stosować zasady netykiety, która jest rodzajem niepisanych, ale przyjętych i przestrzeganych przez internautów zasad korzystania z sieci, m.in. zasad komunikowania się w sieci, jest to rodzaj internetowego savoir-vivre'u. W sieci, tak jak w każdej społeczności, istnieją reguły zachowania się, których należy przestrzegać. Nieprzestrzeganie ich może skutkować uwagami ze strony administratora i innych użytkowników, wykluczeniem z grupy, a nawet całkowitym zablokowaniem dostępu do usług"[49].

Należy zwracać uwagę na to, aby korzystając z Internetu, sprawdzać „tzw. szyfrowanie, które służy do zachowania poufności danych. Plik lub przesyłane dane są zniekształcane tak, że tylko właściwe osoby posiadające tajny «klucz» mogą odtworzyć oryginalny tekst. Gdy ktoś korzysta z urządzeń cyfrowych, cały czas używa systemów opartych na szyfrowaniu: kiedy korzysta z bankowości internetowej, łączy się z siecią Wi-Fi, płaci kartą płatniczą. Wokół prawie każdej czynności w sieci pojawia się szyfrowanie. Dlatego korzystając z poczty, banku lub sklepu internetowego oraz wszystkich stron, na których podaje się swoje dane (login i hasło), należy sprawdzać, czy połączenie jest szyfrowane. Połączenie szyfrowane jest wtedy, gdy w pasku adresu znajduje się kłódka i napis: https «S» oznacza *secur*e, czyli bezpieczny"[50].

Warto pamietać, aby „urządzenia elektroniczne, z których korzystamy, chronić odpowiednim oprogramowaniem ułatwiającym identyfikację zagrożenia wirusowego i pozwalającym te wirusy skutecznie zwalczać. Wirusy infekują urządzenie, gdy ktoś otwiera pocztę od nieznajomych. Najczęściej są to załączniki, które wcale mogą nie wyglądać groźnie. Cyberprzestępcy podszywają się także pod różne instytucje i organizacje. Niebezpieczne jest pobieranie plików z nielegalnie

[47] Z. Polak, *Dorastanie online w czasach koronawirusa*, „Świat Problemów" 2020, nr 6, s. 11–15.
[48] C. Atelak, *E-transformacja przemocy rówieśniczej*, „Dyrektor Szkoły" 2020, nr 12, s. 80–81.
[49] P. Kaca, *Hejt i patostreaming w przestrzeni internetowej*, „Niebieska Linia" 2020, nr 5, s. 24–26.
[50] A. Szuster-Kowalewicz, *Ja tylko klikam?*, „Charaktery" 2020, nr 2, s. 34–38.

rozpowszechnionymi filmami, grami, programami, aplikacjami, książkami, a niekiedy także z muzyką. Instalując nowe oprogramowanie, nie należy klikać w link w wyskakującym okienku z informacją, aby pilnie coś zainstalować. Takie wyskakujące okienka często są pułapką. Linki, które są w nich zawarte, uaktywniają ściągnie na urządzenie pliku ze złośliwym oprogramowaniem"[51].

Bibliografia

1. Atelak C., *E-transformacja przemocy rówieśniczej*, „Dyrektor Szkoły" 2020, nr 12.
2. Banasik K., *Głos w dyskusji o art. 200a k.k.*, „Palestra" 2010, nr 3.
3. Beisert M., Izdebska A., *Wykorzystanie seksualne dzieci*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2012, nr 39(2).
4. Ben-Ze'ev A., *Miłość w sieci. Internet i emocje*, przekł. A. Zdziemborska, Poznań 2005.
5. Bębas S., *Bezpieczeństwo w cyberświecie* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
6. Bębas S., *Cyberprzemoc jako przejaw współczesnej patologii społecznej w świecie wirtualnym* [w:] K. Marzec-Holka, K. Mirosław-Nawrocka, J. Moleda (red.), *Współczesne uwarunkowania i wzory procesów resocjalizacji, reintegracji, inkluzji*, Warszawa 2014.
7. Bębas S., *Cyberprzemoc* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
8. Bębas S., *Cyberprzestępczość* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
9. Bębas S., *Cyberprześladowanie* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
10. Bębas S., *Cyberseks* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
11. Bębas S., *Cyberstalking – wybrane problemy prawne i pedagogiczne* [w:] R. Frey (red.), *Przemiany prawa publicznego i prywatnego na początku XXI wieku*, Kielce 2012.
12. Bębas S., Jasiuk E., *Pedofilia i pornografia w Internecie – wybrane aspekty pedagogiczne i prawnomiędzynarodowe* [w:] J. Bukała, K. Wątorek (red.), *Stop pedofilii*, Kielce 2012.

[51] Ł. Wojtasik, *Wpływajmy na wybory dzieci w Internecie*, „Świat Problemów" 2019, nr 9, s. 21–23.

13. Bębas S., Konopka T., *Selected aspects of security and risks in cyberspace* [w:] G. Sobolewski, A. Cyran (red.), *The practical and theoretical approach to the issue of security*, Kielce 2013.
14. Bębas S., *Krzywdzenie dziecka w sieci – wybrane aspekty profilaktyki* [w:] J. Bukała, K. Wątorek (red.), *Krzywdzenie dziecka – zapobieganie przemocy*, Kielce 2013.
15. Bębas S., *Patologie i zagrożenia w świecie wirtualnym* [w:] S. Bębas, J. Plis, J. Bednarek (red.), *Patologie w cyberświecie*, Radom 2012.
16. Bębas S., *Patologie społeczne w sieci*, Toruń 2013.
17. Bębas S., *Uwodzenie dzieci przez Internet* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
18. Bębas S., *Uzależnienie od komputera, Internetu* [w:] K. Zajdel, M. Prokosz (red.), *Słownik. Kompendium wiedzy nauczyciela i rodzica*, Toruń 2014.
19. Białecka B., *Jak radzić sobie z cyberprzemocą?*, „Wychowawca" 2019, nr 11.
20. Białecka B., *Niebezpieczne zachowania w Internecie*, „Wychowawca" 2019, nr 9.
21. Cent J., *Nowe media a dzieci – dylemat rodziców* [w:] M. Bogunia-Borowska (red.), *Dziecko w świecie mediów i konsumpcji*, Kraków 2006.
22. Chmielecka J., *Internet złych rzeczy*, Bielsko-Biała 2017.
23. Chochowska A., Chochowski K., *Bezpieczeństwo lotnictwa cywilnego wobec zagrożenia terroryzmem* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa transportu lotniczego*, Warszawa 2021.
24. Corbett D., *Let's talk about sext. The challenge of finding the right legal response to the teenage practice of 'sexting'*, „Journal of Internet Law" 2009, nr 12.
25. Cronin B., Davenport E., Zones E., *Positioning pornography in the digital economy*, „The Information Society" 2001, nr 17(1).
26. Dąbrowska M., *Grooming: wybrane aspekty prawnokarne i kryminologiczne*, Warszawa 2018.
27. Fenik K., *Grooming. Uwodzenie dzieci w Internecie* [w:] A. Jodko (red.), *Tabu seksuologii*, Warszawa 2008.
28. Filar M., *Pornografia. Studium z dziedziny polityki kryminalnej*, Toruń 1977.
29. Gołębiewska I., *Cyberprzemoc – zagrożenie dla młodego pokolenia*, „Wychowawca" 2010, nr 7/8.
30. Gregorek A., *Mindfulness – trening uważności dzieci i młodzieży w profilaktyce cyberprzemocy*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1.
31. Heynemann F.C., *Seksting i grooming*, „Dyrektor Szkoły" 2015, nr 6.
32. Hinduja S., Patchin J.W., *Cyberbullying: Neither an epidemic nor a rarity*, „European Journal of Developmental Psychology" 2012, nr 9(5).
33. Hofman Y., Demchuk A., *Kwestie bezpieczeństwa transportu lotniczego w ustawodawstwie Ukrainy* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa transportu lotniczego*, Warszawa 2021.

34. Hudson H.K., *Factors affecting sexting behaviors among selected undergraduate students*, Charleston 2006.
35. Jankowska M.M., *Psychoedukacja rodziców na temat cyberprzemocy*, „Głos Pedagogiczny" 2020, nr 115.
36. Jasiuk E., Konert A., Detyniecka A., Targońska E., *The responsibility of a State in the shooting down of Malaysian Airlines flight MH17*, „Transportation Research Procedia" 2019, vol. 43.
37. Jasiuk E., Marchwińska A., *Terroryzm lotniczy a ochrona praw jednostki zagwarantowana w Europejskiej konwencji praw człowieka* [w:] E. Jasiuk, K. Sikora (red.), *Prawne aspekty bezpieczeństwa transportu lotniczego*, Warszawa 2021.
38. Jasiuk E., Szarpak A., Zielinski R., Madziala M., *Organization of technical rescue operations in the national rescue system,* „Disaster and Emergency Medicine Journal" 2019, vol. 4, nr 2.
39. Jasiuk E., Wosiek R., *Global security and safety management in Civil Aviation in light of Annnex 19 to the Chicago Convention* [w:] E. Jasiuk, R. Wosiek (red.), *Legal conditions of international cooperation for the safety and efficiency of civil aviation*, Warszawa 2019.
40. Kaca P., *Hejt i patostreaming w przestrzeni internetowej*, „Niebieska Linia" 2020, nr 5.
41. Kałuba-Korczak A., *Dziecko w internecie – zagrożenia*, „Wychowanie w Przedszkolu" 2017, nr 5.
42. Kolek A., *Zachowania dyssocjalne młodzieży w przestrzeni internetowej. Implikacje pedagogiczne*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1.
43. Kopaliński W., *Słownik wyrazów obcych i zwrotów obcojęzycznych z almanachem*, Warszawa 1999.
44. Kowalski R., Limber S., *Electronic bullying among middle school students*, „Journal of Adolescent Health" 2007, nr 41.
45. Krajewska M., *Cyberprzemoc w kontaktach rówieśniczych*, „Opieka, Wychowanie, Terapia" 2010, nr 1/2.
46. Krawulska-Ptaszyńska A., *Psychospołeczne uwarunkowania korzystania z pornografii przez mężczyzn*, Poznań 2003.
47. Kubala-Kulpińska A., *Seksting czyli wirtualny ekshibicjonizm, który może śledzić cały świat*, „Głos Pedagogiczny" 2015, nr 68.
48. Leśnicka A., *Cyberseks w polskim Internecie – ankieta dla użytkowników czatów erotycznych,* „Seksuologia Polska" 2009, nr 7(1).
49. Lew-Starowicz Z., *Seks w sieci i nie tylko*, Kraków 2003.
50. Lopez J., *Has the Internet unleashed digital drama?*, „Momentum" 2011, vol. 42, nr 4.

51. Lounsbury K., Mitchell K.J., Finkelhor D., *The true prevalence of „sexting". Crimes against children research centre*, 2011 [online:] https://scholars.unh.edu/cgi/viewcontent.cgi?article=1063&context=ccrc [dostęp: 20.08.2023].
52. Lubkina V., Marzano G., *Zapobieganie cyberprzemocy* [w:] J. Lizut (red.), *Zagrożenia cyberprzestrzeni. Kompleksowy program dla pracowników służb społecznych*, Warszawa 2014.
53. Małysz Z., *Agresywność, agresja, przemoc, bullying i cyberbullying jako problemy opiekuńczo-wychowawcze XXI wieku*, „Problemy Opiekuńczo-Wychowawcze" 2018, nr 1.
54. Marker B.S., *Sexting as moral panic. An explanatory study into the media's construction of sexting*, Richmond 2009.
55. Mitchell K.J., Finkelhor D., Jones L.M., Wolak J., *Prevalence and characteristics of youth sexting. A national study*, „Pediatrics" 2012, nr 129.
56. Pawłowska S., *iGen – pokolenie Internetu*, „Remedium" 2019, nr 12.
57. Polak Z., *Dorastanie online w czasach koronawirusa*, „Świat Problemów" 2020, nr 6.
58. Polcyn-Matuszewska S., *Cyberzagrożenia dla dzieci i młodzieży*, „Remedium" 2017, nr 9.
59. Przedlacka A., *Seksualność w Internecie – zagrożenia i korzyści dla rozwoju psychoseksualnego dzieci i młodzieży*, „Meritum" 2019, nr 3.
60. Pyżalski J., *Agresja elektroniczna – wirtualne ciosy, realne rany – cz. I*, „Remedium" 2008, nr 186(9).
61. Pyżalski J., *Agresja elektroniczna – wirtualne ciosy, realne rany – cz. II*, „Remedium" 2008, nr 186(10).
62. Pyżalski J., *Agresja elektroniczna dzieci i młodzieży. Różne wymiary zjawiska*, „Dziecko Krzywdzone" 2009, nr 1(26).
63. Pyżalski J., *Agresja elektroniczna i mobbing elektroniczny w kontekście zaangażowania w stosowanie nowych technologii komunikacyjnych*, „Kwartalnik Pedagogiczny" 2009, nr 4.
64. Pyżalski J., *Agresja elektroniczna wśród 15-latków w Polsce* [w:] K. Okulicz-Kozaryn, K. Ostaszewski (red.), *Promocja zdrowia psychicznego. Badania i działania w Polsce*, Warszawa 2010.
65. Pyżalski J., *Agresja elektroniczna wśród dzieci i młodzieży*, Sopot 2011.
66. Pyżalski J., *Agresja rówieśnicza online i offline wśród gimnazjalistów. Wybrane uwarunkowania i konsekwencje* [w:] B. Szmigielska (red.), *Edukacja w dwóch światach offline i online*, Kraków 2011.
67. Pyżalski J., *Agresja w materiałach publikowanych w Internecie przez użytkowników – flirt tradycyjnych i nowych mediów* [w:] J. Drozdowicz, M. Bernasiewicz (red.), *Kultura popularna w społeczeństwie współczesnym. Teoria i rzeczywistość*, Kraków 2010.

68. Pyżalski J., *Bezpieczny Internet w szkole – jak zapobiegać cyberprzemocy?*, „Głos Pedagogiczny" 2018, nr 97.
69. Pyżalski J., *Cyberbullying – stare wino w nowej butelce* [w:] L. Jakubowska-Malicka, A. Kobylarek, M. Pryszmont-Ciesielska (red.), *Audiowizualność. Cyberprzestrzeń. Hipertekstualność. Ponowoczesne konteksty. Edukacja*, Wrocław 2009.
70. Pyżalski J., *Gimnazjaliści online: dobre i złe wiadomości z polskiej części wyników European Cyberbullying Intervention Project* [w:] J. Pyżalski (red.), *Cyberbullying. Zjawisko, konteksty, przeciwdziałanie*, Łódź 2012.
71. Ronatowicz W., *Ryzykowne zachowania seksualne dzieci, młodzieży i młodych dorosłych w kontekście korzystania z technologii cyfrowych*, „Rocznik Lubelski" 2014, t. 40, cz. 1.
72. Siegle D., *Cyberbullying and sexting. Technology abuses of the 21st century*, „Gifted Child Today" 2010, t. 32, nr 2.
73. Skierkowska M., *Edukacyjne programy profilaktyki wykorzystania seksualnego dzieci*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, nr 13(1).
74. Smith P.K., Mahdavi J., Carvalho M., Fisher S., Russell S., Tippett N., *Cyberbullying: its nature and impact in secondary school pupils*, „Journal of Child Psychology and Psychiatry" 2008, nr 49(4).
75. Szlendak T., *Wielozmysłowa kultura iwentu. Skąd się wzięła, czym się objawia i jak w jej ramach oceniać dobro kultur*, „Kultura Współczesna. Teoria. Interpretacje. Praktyka" 2010, nr 4(66).
76. Szuster-Kowalewicz A., *Ja tylko klikam?*, „Charaktery" 2020, nr 2.
77. Taylor K.R., *„Sexting": fun or felony?*, „Principal Leadership" 2009, vol. 9, nr 8.
78. Temple J.R., Jonathan A.P., Van Den Berg P., Le V.D., McElhany A., Temple B.W., *Teen sexting and its association with sexual behaviors*, „Archives of Pediatrics and Adolescent Medicine" 2012, nr 166(9).
79. Warylewski J., *Reakcja karna na przestępstwa seksualne*, „Przegląd Więziennictwa Polskiego" 2007, nr 54.
80. Willard N.E., *Cyberbullying and cyberthreats. Responding to the challenge of online social aggression, threats, and distress*, San Francisco 2007.
81. Witty M.T., Carr A.N., *Wszystko o romansie w sieci. Psychologia związków internetowych*, przekł. T. Kościuczuk, Gdańsk 2009.
82. Włodarczyk J., Sajkowska M., *Wykorzystywanie seksualne dzieci. Wyniki ogólnopolskiej diagnozy problem przemocy wobec dzieci*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2013, nr 12(3).
83. Wojtas M., *Proces uwodzenia dzieci w Internecie* [w:] *Dziecko w sieci. Zapobieganie wykorzystywaniu seksualnemu dzieci w Internecie. Profilaktyka. Prewencja. Nowa legislacja*, Warszawa 2010.
84. Wojtasik Ł., *Cyberprzemoc*, „Remedium" 2008, nr 2.

85. Wojtasik Ł., *Seksting wśród dzieci i młodzieży*, „Dziecko Krzywdzone. Teoria, Badania, Praktyka" 2014, nr 13(2).
86. Wojtasik Ł., *Wpływajmy na wybory dzieci w internecie*, „Świat Problemów" 2019, nr 9.
87. Young K.S., *Internet addiction: symptoms, evaluation and treatment* [w:] L. Vande Creek, T. Jackson (red.), *Innovations in clinical practice. A source book*, Florida 1999.
88. Юхимюк О., *Особливості викладу принципів права у національному законодавстві*, „Науковий вісник Херсонського державного університету", seria „Юридичні науки", wyd. 6, t. 1, Херсон 2013.
89. Юхимюк О.М., *Сумління (сумлінність) судді в міжнародному та національному праві*, „Експерт: парадигми юридичних наук і державного управління" 2021, nr 5(17).