STUDIA GDAŃSKIE
TOM XXVIII

Małgorzata Gruchoła
Instytut Kulturoznawstwa
Katolicki Uniwersytet Lubelski Jana Pawła II

Ochrona małoletnich internautów jako zadanie i wyzwanie dla rodziny w państwach Unii Europejskiej

Streszczenie: Celem publikacji jest analiza ochrony małoletnich internautów jako zadania i wyzwania rodziców, ponadto weryfikacja działań podejmowanych w tym zakresie przez państwa Wspólnoty, wreszcie próba odpowiedzi na pytanie: czy zaproponowane rozwiązania są skuteczne? Po wstępnych rozważaniach teoretycznych dotyczących mapy zagrożeń przeanalizowano kluczowe dla tytułowej ochrony regulacje prawne. Wdrożenie priorytetów polityki ochrony dokonuje się poprzez realizację programów pomocowych. Jednym z nich jest *Safer Internet*. Zweryfikowano założenia Polskiego Centrum Programu *Safer Internet,* w tym działalność Fundacji Dzieci Niczyje oraz Naukowej i Akademickiej Sieci Komputerowej. Omówiono zadania i inicjatywy projektu *Saferinternet.pl* (m.in. zespół kontaktowy: Dyżurnet.pl, tzw. *hotline* oraz zespół pomocowy, tzw. Helpline.org.pl), cele kampanii medialnych i społecznych (np. „Dziecko w sieci"). Zanalizowano zagadnienie umiejętności korzystania z internetu. Omówiono techniczne urządzenia wspomagające ochronę dzieci. Słowa kluczowe: dzieci, edukacja medialna, inicjatywy, internet, ochrona, prawo, Unia Europejska.

Wprowadzenie

Nie od dziś mówi się o zagrożeniach, jakie niesie ze sobą Internet. Jest to temat poruszany zarówno przez teoretyków jak i praktyków, coraz częściej też przez polityków oraz osoby odpowiedzialne za bezpieczeństwo dzieci. Z raportu *EU Kids Online*[1], zawierającego analizę wyników z 250 badań dotyczących używania Internetu przez dzieci w państwach Unii Europejskiej wynika, że ponad połowa rodziców obawia się kontaktu dziecka z treściami pornograficznymi lub związanymi z przemocą (65% UE, 67% PL); uwodzenia dziecka przez nieznajomych

[1] Raport dostępny na stronie: http://www.lse.ac.uk/collections/EUKidsOnline/ (odczyt z dn. 4 maja 2011 r.).

w globalnej sieci (60% UE, 60% PL); dokuczania dziecku przez rówieśników (54% UE, 56% PL); społecznej izolacji dziecka ze względu na ilość czasu spędzanego przed komputerem (53% UE, 56% PL). Nieco mniej rodziców niepokoi się możliwością przekazania przez dziecko prywatnych informacji (47% UE, 38% PL). Warto zaznaczyć, że tylko co trzecie dziecko (w Polsce i Europie) zwraca się do rodziców o pomoc w trudnej sytuacji związanej z Internetem. W przypadku poważniejszych zagrożeń o pomoc prosi jedynie co 10 dziecko. Jedynie połowa rodziców w Polsce zainstalowała na domowym komputerze program filtrujący lub monitorujący aktywność dziecka w globalnej sieci. 16% badanych rodziców nie potrafi jednak korzystać z tego rodzaju oprogramowania[2].

Jasno i wyraźnie kształtuje się zatem obraz polskiego rodzica, który ma stosunkowo wysoką świadomość zagrożeń, ale często nie dysponuje wystarczającą wiedzą i umiejętnościami, by zadbać o bezpieczeństwo dziecka surfującego w Internecie. Nasuwają się pytania: jakie są rodzaje zagrożeń; jakie są podstawy prawne ochrony małoletnich internautów; jakie działania podejmuje UE w celu zapewnienia ochrony najmłodszym użytkownikom Internetu; co stanowi istotę umiejętności korzystania z Internetu; jakie techniczne urządzenia wspierają ochronę dziecka?

1. Zestawienie zagrożeń

Stosunek do Internetu jest bardzo różnorodny od niemal utopijnego, euforycznego zachwytu, po katastroficzne wizje piętnujące globalną sieć z powodu zagrożeń, jakie ze sobą niesie. Oddziaływanie Internetu można podzielić na dwa rodzaje:

- pośrednie: jest to czas odjęty innym czynnościom, np. komunikowaniu się „twarzą w twarz";
- bezpośrednie: to treści, sposób odbioru i komunikowania[3].

Z jednej strony Internet służy młodym ludziom do celów edukacyjnych pozwalając samodzielnie pogłębiać wiedzę. Z drugiej, daje nieograniczony dostęp także do treści zawierających elementy przemocy, agresji czy erotyzmu. Zatracając się w internetowych grach *on-line* młodzież często traci kontakt z realnym światem, w skrajnych przypadkach może popaść w uzależnienie. W wirtualnym świecie wszyscy są anonimowi, nie ma możliwości zweryfikowania personaliów drugiej osoby. Stąd Internet stał się specyficznym miejscem poszukiwania przez osoby dorosłe kontaktu z dziećmi i areną udostępniania pornografii[4].

[2] Dyżurnet.pl, *Rozwiązania filtrujące niepożądane treści w internecie. Raport Dyżurnet.pl*, Warszawa 2009, s. 4.

[3] *Tamże,* s. 75.

[4] K. Śpiewak, *Internet a zagrożenia rozwoju dzieci i młodzieży*, w: *Jednostka – grupa – cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*, red. M. Radochoński, B. Przywara, Rzeszów 2004, s. 104.

Jednak cybersieć to nie tylko zagrożenia psychiczne, ale i fizyczne. Zbyt długie przesiadywanie przed komputerem w nieprawidłowych pozycjach prowadzi do skrzywień kręgosłupa i innych wad postawy, wad wzroku, a także uszkodzenia nerwów odpowiedzialnych za ruchy nadgarstka i dłoni.

Z punktu ochrony dziecka-internauty należy wyróżnić zagrożenia związane z treściami w Internecie oraz wynikające z utrzymywania kontaktów przez globalną sieć[5]. W obydwu grupach część zagrożeń wynika z zachowania samych użytkowników Internetu, pozostałe – ze sposobu postępowania innych. Istnieją też zagrożenia, których przypisanie do jednego z dwu wymiarów, wynika z przyjętej perspektywy – konsumenta lub producenta, szczególnie w przypadku treści generowanych przez użytkownika. Przypadek ten pokazuje, że te dwa wymiary wzajemnie się przenikają.

Do pierwszej grupy zagrożeń zalicza się między innymi treści: nieodpowiednie dla określonych grup wiekowych, zawierające przemoc, niezgodne z prawdą i prawem: rasizm, ksenofobię, pornografię dziecięcą, zachęcające do autoagresji, naruszające prawa człowieka i jego godność. Ponadto są: nieadekwatna reklama i działania marketingowe skierowane do dzieci, utrwalanie i przenoszenie danych oraz naruszanie praw autorskich[6]. Uzasadnienie *Rekomendacji* Komitetu Ministrów Rady Europy z dnia 31 października 2001 r. daje wykładnię treści nielegalnych oraz szkodliwych. Pierwsze to treści sprzeczne z prawem krajowym. Treści szkodliwe ujmuje jako niekoniecznie nielegalne, za to potencjalnie niosące szkodę, szczególnie dla fizycznego, psychicznego i moralnego rozwoju małoletnich[7]. Przykładami są treści propagujące ruchy religijne uznane za sekty, przedstawiające anoreksję i bulimię jako styl życia, a nie poważną chorobę, nawołujące do samookaleczeń, promujące narkotyki i inne używki, środki farmaceutyczne, takie jak: tabletki gwałtu, dopalacze lub sterydy. Nowym zagrożeniem ze strony globalnej sieci są tzw. dziecięce pokoje śmierci. W Internecie istnieje obecnie ponad 9000 stron internetowych, na których inni ludzie nakłaniają

[5] Stiftung Digitale Chancen, *Zestaw zaleceń projektu Youth Protection Roundtable*, Hamburg 2009, s. 7.

[6] J. Śpiewak, *Wykorzystanie seksualne dziecka w kodeksie karnym*, „Niebieska Linia" 2010, nr 3, s. 28–37; Ł. Wojtasik, *Pedofilia i pornografia dziecięca w internecie*, „Dziecko Krzywdzone" 2003, nr 2, s. 56 – 67; J. Tęcza-Ćwierz, *Internet – szanse i zagrożenia,* „Wychowawca" 2003, nr 6, s. 16–17; K. Paradowski, *Internet: korzyści, zagrożenia: praktyczny poradnik dla nauczycieli, pedagogów, rodziców,* Warszawa 2000; T. Palmer, *Ciemna strona internetu – ofiary pornografii dziecięcej,* „Dziecko Krzywdzone" 2005, nr 13, s. 28–44; I. R. Berson, *Cyberofiary: psychospołeczne konsekwencje wykorzystywania młodzieży za pośrednictwem internetu*, „Dziecko Krzywdzone" 2003, nr 2, s. 72–83; M. Kordoń, *Niebezpieczeństwa sieci*, „Psychologia w Szkole" 2004, nr 2, s. 55–63; M. Braun-Gałkowska, *Oddziaływanie internetu na psychikę dzieci*, „Edukacja Medialna" 2003, nr 3, s. 14–20; W. Wosińska, *Terror z komputerów*, „Charaktery" 2005, nr 7, s. 25–26.

[7] Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)8 z dnia 31 października 2001 r. dotycząca samoregulacji w zakresie cyberzawartości: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych, http://www.krrit.gov.pl/bip/Portals/0/publikacje/analizy/Analiza2005_07.pdf (odczyt z dn. 6 maja 2011 r.).

do samobójstwa, podają sposoby jego popełnienia czy szukają towarzysza, który razem z nim targnie się na swoje życie.

Drugą grupę stanowią zagrożenia związane z kontaktowaniem się przez Internet. Zalicza się do nich: wykluczenie społeczne i cyfrowe, szkodliwe porady, uzależnienie od globalnej sieci, kradzież tożsamości, poufnych danych lub pieniędzy (*phishing*), oszustwo handlowe, ujawnianie prywatnych informacji oraz pozyskiwanie danych z profili internetowych[8]. Ponadto podczas korzystania z Internetu dzieci mogą się zetknąć z niepokojącymi zjawiskami, takimi jak:

- *cyberbullying* – forma przemocy polegająca na wyzywaniu, ośmieszaniu, szantażowaniu czy rozprzestrzenianiu kompromitujących materiałów w sieci przy użyciu technologii informacyjnych i komunikacyjnych (komunikatorów, czatów, stron www, blogów)[9];
- *grooming* – uwodzenie dzieci przez osoby dorosłe za pomocą Internetu. Do nawiązywania bliskiego kontaktu z małoletnimi „cyberłowcy" wykorzystują głównie komunikatory internetowe oraz czaty. Starają się oni nakłonić dzieci do rozmów o seksie, co może być wstępem do dalszego ich osaczania i molestowania. Dorosły, często udając rówieśnika swej ofiary, stopniowo zdobywa jej zaufanie, dane osobowe, zdjęcia, a często staje się jej „dobrym przyjacielem". Namawia dziecko do oglądania pornografii i nalega na spotkanie w świecie rzeczywistym. Gdy dojdzie do spotkania, dziecko zazwyczaj zostaje wykorzystane seksualnie i nierzadko staje się ofiarą przemysłu pornograficznego[10].

---

[8] K. Fenik, *Uzależnienie od internetu. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie*; Warszawa 29.–30.09.2009 r. Materiały niepublikowane; S. Kosek-Nita, *Uzależnienie od komputera i jego następstwa*, „Wychowanie na Co Dzień" 2006, nr 3, s. 6–9; C. Guerreschi, *Nowe uzależnienia*, Kraków 2006; M. Maj, *Techniczne aspekty bezpieczeństwa w internecie. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29.–30.09.2009r. Materiały niepublikowane; M. Serzycki, *Portale społecznościowe a ochrona danych osobowych. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29.–30.09.2009r. Materiały niepublikowane.

[9] J. Wolak, K. Mitchell, D. Finkelhor, *Czy nękanie za pośrednictwem internetu jest formą przemocy rówieśniczej? Analiza zjawiska nękania online przez znajomych rówieśników i przez sprawców znanych wyłącznie z sieci*, „Dziecko Krzywdzone" 2009, nr 29, s. 77–89; M. Walrave, W. Heirman, *Skutki cyberbullyingu – oskarżenie czy obrona technologii?*, „Dziecko Krzywdzone" 2009, nr 29, s. 27–36; J. Pyżalski, *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska*, „Dziecko Krzywdzone" 2009, nr 29, s. 12- 26; Ł. Wojtasik, *Przemoc rówieśnicza z użyciem mediów elektronicznych*, „Dziecko Krzywdzone" 2009, nr 29, s. 7–11; H. Hrpka, *Chorwackie działania na rzecz zapobiegania przemocy wobec dzieci w internecie*. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie; Warszawa 29.–30.09.2009r. Materiały niepublikowane.

[10] O. Levina, *Pomoc ofiarom wykorzystywania seksualnego przez internet w Rosji. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29.–30.09.2009r. Materiały niepublikowane.

2. Ochrona dzieci i młodzieży przez prawo Unii Europejskiej i Rady Europy

Prawną podstawę ochrony dzieci i młodzieży zapewnia przyjęty w 1999 roku[11] i kontynuowany na mocy kolejnych Decyzji Parlamentu Europejskiego i Rady wieloletni plan działań Wspólnoty w zakresie promowania bezpieczniejszego korzystania z Internetu poprzez zwalczanie sprzecznych z prawem i szkodliwych treści w światowych sieciach komputerowych: *Safer Internet Action Plan*, *Safer Internet Plus* na lata 2005–2008 oraz *Safer Internet 2009–2013*[12]. Ponadto *Dyrektywa 2010/13/UE o audiowizualnych usługach medialnych z 2010 r.*[13], zalecająca podjęcie działań na rzecz przeciwdziałania analfabetyzacji medialnej dzieci i młodzieży. Dla tytułowej ochrony kluczowe znaczenie mają:

- *Konwencja Rady Europy o Cyberprzestępczości z dnia 23 listopada 2001 r*[14];
- *Decyzja Ramowa Rady Unii Europejskiej 2004/68/WSiSW dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej z dnia 22 grudnia 2003 r*[15];
- *Konwencja Rady Europy z dnia 12 lipca 2007 r. o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych*[16].

Katalog regulacji związanych z pornografią dziecięcą zawiera uchwalona przez Radę Europy w 2001 roku *Międzynarodowa Konwencja o Cyberprzestępczości*, w której znalazły się nowe kategorie przestępstw związanych z produkowaniem, oferowaniem, udostępnianiem, rozpowszechnianiem, transmitowaniem, posiadaniem oraz pozyskiwaniem pornografii dziecięcej za pomocą systemów informatycznych (art. 9 ust. 1)[17]. Pornografia dziecięca – zgodnie z art. 9 – obejmuje materiał pornograficzny, który w sposób widoczny przedstawia w trakcie czynności wyraźnie seksualnej: osobę małoletnią; osobę, która

[11] Decyzja nr 276/1999/WE Parlamentu Europejskiego i Rady z dnia 25 stycznia 1999 r. przyjmująca wieloletni plan działań Wspólnoty w zakresie promowania bezpieczniejszego korzystania z Internetu poprzez zwalczanie sprzecznych z prawem i szkodliwych treści w sieciach komputerowych, Dz. Urz. L 33 z 06.02.1999.

[12] Decyzja nr 1351/2008/EC Parlamentu Europejskiego i Rady z dnia 24 grudnia 2008 r. w sprawie kontynuacji wieloletniego programu wspólnotowego na rzecz bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych, Dz. Urz. L 348, 24.12.2008.

[13] Dyrektywa 2010/13/UE Parlamentu Europejskiego i Rady z dnia 10 marca 2010 r. o audiowizualnych usługach medialnych), Dz. Urz. L 95/22 z 15.04.2010.

[14] Konwencja Rady Europy o Cyberprzestępczości z dnia 23 listopada 2001 r., http://www.ms.gov.pl/ue/ue3in32.shtml (odczyt z dn. 7 maja 2011 r.).

[15] Decyzja Ramowa Rady 2004/68/WSiSW z dnia 22 grudnia 2003 r. dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej, Dz. Urz. L 013 z 20.01.2004.

[16] Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych z dnia 12 lipca 2007 r., http://www.ms.gov.pl/re/081027_konw.pdf (odczyt z dn. 3 maja 2011 r.).

[17] Konwencja Rady Europy o Cyberprzestępczości z dnia 23 listopada 2001 r., art. 9.

wydaje się być małoletnią oraz realistyczny obraz przedstawiający małoletniego. Pojęcie „osoba małoletnia" obejmuje wszystkie osoby poniżej 18. roku życia. Strona może wprowadzić wymóg niższej granicy wieku, która nie może być niższa niż 16 lat[18]. Natomiast art. 23 *Konwencji Rady Europy z* 2007 roku wprowadza karalność tzw. *groomingu*[19].

O ile konwencje Rady Europy są dokumentami o charakterze fakultatywnym, *Decyzja Ramowa Rady Unii Europejskiej z 2003 roku dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej* ma charakter obligatoryjny dla państw członkowskich UE. Zobowiązała ona państwa do podjęcia niezbędnych środków, gwarantujących poddanie karze następujących czynów popełnionych umyślnie: zmuszanie dziecka do prostytucji lub udziału w przedstawieniach pornograficznych, czerpanie z tego zysku albo wykorzystywanie dziecka w inny sposób do takich celów jak: uczestniczenie w czynnościach o charakterze seksualnym (z użyciem przymusu, siły lub groźby, w zamian za pieniądze lub inną formę wynagrodzenia jako opłaty za udział dziecka w takich czynnościach, poprzez wykorzystanie zaufania, władzy lub wpływu na dziecko). Ponadto została poddana karze, także dokonana z wykorzystaniem systemu komputerowego, produkcja, dystrybucja, rozpowszechnianie, przesyłanie, dostarczanie, udostępnianie, nabywanie lub posiadanie materiałów z pornografią dziecięcą. W 2008 roku wszystkie państwa UE posiadały takie przepisy prawne.

W celu harmonizacji międzynarodowego prawa w omawianym zakresie (np. w Austrii karane było tylko posiadanie, dozwolone oglądanie), w 2009 roku dokonano nowelizacji *Decyzji Ramowej*. Główny nacisk został położony na podniesienie standardów ochrony dzieci, w tym wprowadzenie przepisów prawnych regulujących zjawisko uwodzenia małoletnich w sieci (*grooming*). Znowelizowana *Decyzja* zobowiązuje państwa UE do działań na trzech płaszczyznach: ścigania przestępców, chronienia ofiar i prewencji. Ułatwia karanie sprawców nadużyć seksualnych wobec dzieci poprzez ustanowienie sankcji karnych wobec nowych form nadużyć, takich jak: „nagabywanie nieletnich w celach seksualnych", przeglądanie pornografii dziecięcej bez pobierania plików na własny komputer oraz zmuszanie dzieci do pozowania o charakterze seksualnym przed kamerą internetową. Pokrzywdzone osoby mogą składać zeznania bez konieczności konfrontacji ze sprawcą w sądzie, aby oszczędzić im dodatkowych traumatycznych przeżyć. Mają zapewnioną bezpłatną pomoc prawnika. Opracowano również systemy blokujące dostęp do stron internetowych z pornografią dziecięcą[20].

[18] *Tamże*.

[19] Decyzja Ramowa Rady 2004/68/WSiSW z dnia 22 grudnia 2003 r. dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej, Dz. Urz. L 013 z 20.01.2004, art. 23.

[20] *Inicjatywy i raporty Komisji Europejskiej. Sprawozdanie nr 21/2009,* http://www.senat.gov.pl/k7/ue/inne/2009/021.pdf (odczyt z dn. 15 maja 2011 r.).

Dla tytułowej ochrony istotne, aczkolwiek niesprawcze znaczenie mają rekomendacje i zalecenia Parlamentu Europejskiego oraz Rady Europy[21]. Wymienione dokumenty proponują: opisy narzędzia dostępu warunkowego, system mediacji i arbitrażu, odpowiedzialność karną operatorów platform dyskusyjnych, tzw. *czatów* oraz forów internetowych o charakterze pedofilskim; usuwanie z Internetu nielegalnych materiałów przedstawiających wykorzystywanie dzieci u źródła ich rozpowszechniania; wprowadzenie funkcjonalnej domeny głównej *(Generic Top Level Domaine)* zarezerwowanej dla stron stale kontrolowanych, których administratorzy zobowiązaliby się do poszanowania małoletnich i ich praw, pod rygorem sankcji karnych (np. domena „KID"). Ponadto zalecają współpracę państw członkowskich z dostawcami Internetu, w celu likwidowania stron www wykorzystywanych do popełniania czynów uznanych za przestępcze; zamknięcie lub zablokowanie systemu płatności przez Internet za sprzedaż przez sieć pornografii dziecięcej; zachęcanie podmiotów gospodarczych (banki, kantory wymiany walut) do zwalczania pornografii dziecięcej; zapewnienie rodzicom programów i innych urządzeń technicznych umożliwiających zablokowanie dostępu ich dzieci do internetowych stron pornograficznych. Rada Europy zaleca także współpracę państw członkowskich z sektorem prywatnym, organizacjami społecznymi w celu przyjęcia i realizowania spójnej strategii ochrony dzieci przed zagrożeniami w Internecie, a jednocześnie zachęca, by popierały ich aktywne uczestnictwo w społeczeństwie informacyjnym. Natomiast Komisja Europejska zachęca do współpracy w wymianie doświadczeń i dobrych praktyk pomiędzy organami samoregulującymi oraz współregulującymi zajmującymi się oceną lub klasyfikacją treści internetowych. Celem współpracy jest umożliwienie, szczególnie rodzicom, zgłaszania treści nielegalnych, a także treści legalnych, które mogłyby szkodzić fizycznemu lub umysłowemu rozwojowi dzieci.

Jak wcześniej wspomniałam, obecnie wszystkie państwa członkowskie UE przyjęły przepisy prawne chroniące małoletnich, w tym głównie zabraniające posiadania, produkcji, czy dystrybucji materiałów o charakterze pornografii dziecięcej w globalnej sieci. W stosunku do innych form działań pedofilów w Internecie niewiele krajów przyjęło odpowiednie przepisy prawne. Liczne kontrowersje budzi kwestia zakazu oglądania pornografii dziecięcej. Przepisy formułujące taki zakaz, uznawane są często za ograniczające podstawowe wolności, a mechanizmy kontroli (np. dostęp do zasobów komputerowych) za niedopuszczalne naruszanie prywatności.

[21] Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)8 z dnia 31 października 2001 r.; Zalecenie Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie ochrony małoletnich, godności ludzkiej oraz prawa do odpowiedzi w odniesieniu do konkurencyjności europejskiego przemysłu audiowizualnego oraz internetowych usług informacyjnych, Dz. Urz. L 378 z 27.12.2006; Zalecenie Parlamentu Europejskiego dla Rady z dnia 3 lutego 2009 r. w sprawie walki z seksualnym wykorzystywaniem dzieci i pornografią dziecięcą, Dz. Urz. L. 12 z 03.02.2009; Zalecenie Rady Europy Rec(2009)5 z dnia 8 lipca 2009 r. w sprawie ochrony dzieci przed szkodliwymi treściami i zachowaniami oraz promowania ich aktywnego uczestnictwa w nowym środowisku informacyjnym i komunikacyjnym, Dz. Urz. L. 29 z 08.07.2009.

3. Ochrona dzieci przez polskie prawo

W art. 72 ust. 1 Konstytucji RP zawarta jest norma dotycząca ochrony dziecka przed przemocą, okrucieństwem, wyzyskiem i demoralizacją. Gwarantem jej wypełnienia jest państwo oraz organy władzy państwowej[22]. *Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego*[23], uznaje zdrowie psychiczne za „fundamentalne dobro osobiste, którego ochronę winny zapewnić organy administracji rządowej i samorządowej, a także instytucje do tego powołane" (preambuła). Gwarantem wypełnienia tego zadania jest państwo oraz organy władzy państwowej. Podpisana przez Polskę w 1991 roku *Konwencja o Prawach Dziecka* stanowi najobszerniejszy katalog ich praw[24]. Zadania związane z ochroną przed rosnącą dostępnością pornografii dziecięcej w Internecie nakłada *Protokół Opcjonalny do Konwencji o Prawach Dziecka z 2000 roku*[25].

Obowiązujące polskie prawo karne nie definiuje w ogóle „treści pornograficznych". Zgodnie z prawem krajowym, karalny jest każdy kontakt o charakterze seksualnym z osobą, która nie ukończyła 15. roku życia (art. 200 §1 k.k.)[26]. Nowela z 2005 roku zrównała dobrowolny kontakt seksualny z dzieckiem z gwałtem. Polskie prawo przewiduje karalność rozpowszechniania, a także posiadania, przechowywania, utrwalania, produkowania i sprowadzania w celu rozpowszechniania treści pornograficznych z udziałem osoby poniżej 15. roku życia.

Ideą zmian prawnych, które uchwalił polski rząd w 2009 roku, było dostosowanie prawa polskiego *do Decyzji Ramowej Rady UE z 2003 roku, dotyczącej zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej*[27]. Nowelizacja polskiego prawa[28] wprowadziła przepisy umożliwiające skuteczne zwalczanie wykorzystywania seksualnego dzieci w Internecie, zgodne z wcześniej wymienionymi dokumentami międzynarodowymi. Dodano w art. 202 kodeksu karnego §4b w brzmieniu: „Kto produkuje, rozpowszechnia, prezentuje, przechowuje lub posiada treści pornograficzne przedstawiające wytworzony albo przetworzony wizerunek małoletniego uczestniczącego w czynności seksualnej podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności

[22] Konstytucja Rzeczypospolitej Polskiej; Ustawa z dnia 2 kwietnia 1997 r., Dz. U. z 1997 r. Nr 78, poz. 483, art. 72.

[23] Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego, Dz. U. z 1994 r. Nr 111, poz. 535, art. 4.

[24] Konwencja o Prawach Dziecka z dnia 20 listopada 1989 r. Ustawa w sprawie ratyfikacji Konwencji o Prawach Dziecka z dnia 20 listopada 1989 r., Dz. U. z 1991 r. Nr 120, poz. 526.

[25] Protokół Opcjonalny do Konwencji Narodów Zjednoczonych o Prawach Dziecka dotyczący sprzedaży dzieci, prostytucji dziecięcej i pornografii z udziałem dzieci z dnia 25 maja 2000 r., http://www.vilp.de/p11.htm (odczyt z dn. 8 maja2011 r.).

[26] Kodeks karny; Ustawa z dnia 6 czerwca 1997 r., Dz. U. z 1997 r. Nr 88, poz. 553 ze zm., art. 200.

[27] Decyzja Ramowa Rady Unii Europejskiej 2004/68/WSiSW z dnia 22 grudnia 2003 r.

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

do lat 2". Przepis ten dotyczy problemu pornografii wytworzonej z udziałem dzieci lub wykorzystującej wizerunek dziecka, będący efektem np. animacji komputerowej. Przed nowelizacją ściganie produkcji tego typu obrazów, często o ewidentnie pornograficznym charakterze, nie miało podstawy prawnej. Także na mocy powyższej nowelizacji w art. 101 kodeksu karnego zmianie uległ czas przedawnienia przestępstw o charakterze seksualnym wobec małoletniego. Przedawnienie nie może obecnie nastąpić przed upływem 5 lat od ukończenia przez pokrzywdzonego 18 roku życia. Wcześniej, dla poszczególnych przestępstw termin przedawnienia był określony odrębnie, tj. od momentu popełnienia przestępstwa[29]. Ponadto nowelizacja zaostrza kary za pedofilię – zgwałcenie małoletniego traktowane jest jako zbrodnia. Wprowadza nowe czyny zabronione (np. nagabywanie dzieci przez Internet czy propagowanie pedofilii), zwiększa uprawnienia Policji w zakresie ścigania pedofilów (zezwala na stosowanie działań operacyjnych), a także usprawnia wykonywanie kar (przymusowa terapia przestępców).

Prawo mówi wyraźnie o obcowaniu płciowym lub „innej czynności seksualnej"[30]. Można za taką uznać również tzw. cyberseks, czyli wirtualną rozmowę na tematy seksualne, która służy zaspokojeniu popędu seksualnego sprawcy. Z punktu widzenia prawa nie ma znaczenia, czy dziecko wyraziło zgodę na kontakty seksualne. Tłumaczenia sprawców, że „ono samo tego chciało", czy „myślałem, że mam do czynienia z osobą starszą" nie mają w zasadzie żadnej wagi, choć w przypadku, gdy wygląd dziecka może wprowadzać w błąd, co do jego wieku, sąd może potraktować to jako okoliczność łagodzącą[31].

W *Kodeksie karnym* (art. 200a)[32] pojawił się zupełnie nowy rodzaj przestępstwa – *grooming*. Karze będzie podlegać osoba, która np. za pośrednictwem

---

[29] R. Lew-Starowicz, *Nowe rozwiązania legislacyjne w zakresie zwalczania pedofilii i pornografii dziecięcej w internecie,* Warszawa 2009, s. 30.

[30] *Kodeks karny*…, art. 200: „Kto obcuje płciowo z małoletnim poniżej lat 15 lub dopuszcza się wobec takiej osoby innej czynności seksualnej lub doprowadza ją do poddania się takim czynnościom albo do ich wykonania, podlega karze pozbawienia wolności od lat 2 do 12 (§1). Tej samej karze podlega, kto w celu zaspokojenia seksualnego prezentuje małoletniemu poniżej lat 15 wykonanie czynności seksualnej"(§2).

[31] J. Śpiewak*, Wykorzystanie seksualne dziecka w kodeksie karnym,* „Niebieska Linia" 2010, nr 3, s. 28–37; J. Śpiewak, Aspekty prawne, http://www.kidprotect.pl/artykuly/?item=1 (odczyt z dn. 3 maja 2011 r.).

[32] *Kodeks karny*…, art. 200a: „Kto w celu popełnienia przestępstwa określonego w art. 197 § 3 pkt 2 lub art. 200, jak również produkowania lub utrwalania treści pornograficznych, za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej nawiązuje kontakt z małoletnim poniżej lat 15, zmierzając, za pomocą wprowadzenia go w błąd, wyzyskania błędu lub niezdolności do należytego pojmowania sytuacji albo przy użyciu groźby bezprawnej, do spotkania z nim, podlega karze pozbawienia wolności do lat 3 (§1.). Kto za pośrednictwem systemu teleinformatycznego lub sieci telekomunikacyjnej małoletniemu poniżej lat 15 składa propozycję obcowania płciowego, poddania się lub wykonania innej czynności seksualnej lub udziału w produkowaniu lub utrwalaniu treści pornograficznych, i zmierza do jej realizacji, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2" (§2).

Internetu (na wszelkiego rodzaju forach internetowych, czatach, przy pomocy komunikatorów internetowych) albo telefonii komórkowej nawiązuje kontakt z dzieckiem poniżej lat 15 i działając w celu popełnienia przestępstwa zgwałcenia, molestowania seksualnego lub produkowania i utrwalania pornografii dziecięcej podejmuje działania zmierzające do spotkania lub realizacji tego celu w innej formie. Wcześniej Policja mogła podejmować działania tylko wtedy, gdy doszło do molestowania seksualnego dziecka. Nowe prawo pozwala nie tylko zareagować, ale i karać zanim dziecko zostanie skrzywdzone. Co ważne – Policja otrzymała uprawnienia do stosowania działań operacyjnych w takich sprawach[33]. W *Kodeksie karnym* pojawia się jeszcze jeden nowy typ przestępstwa, jakim jest publiczne (np. w Internecie) pochwalanie lub propagowanie zachowań o charakterze pedofilskim[34]. Strony www, na których pojawią się wypowiedzi sugerujące, że obcowanie płciowe z dziećmi jest zjawiskiem pozytywnym, stają się nielegalne, a ich twórcy mogą zostać pociągnięci do odpowiedzialności karnej[35].

Polskie prawo nie delegalizuje pornografii jako takiej. Wprowadza jednak zasadę, że treści tego rodzaju mają być rozpowszechniane w taki sposób, by nie narażało to na kontakt z nimi osób, które sobie tego nie życzą (np. dzieci)[36]. Oznacza to, że nie musi dojść do faktycznego narzucenia odbioru, nie jest potrzebna skarga osoby, która wbrew swojej woli została narażona na kontakt z pornografią. Wystarczy fakt nieskutecznego jej zabezpieczenia przez osobę publicznie prezentującą[37]. Przestępstwo, o którym mowa w art. 202 §1 jest ścigane na wniosek pokrzywdzonego. W praktyce internetowej można uznać, że strona, której opis w wyszukiwarce lub adres wprowadza w błąd, poprzez ukrycie jej pornograficznego charakteru, może zostać uznana za sprzeczną z prawem. Podobnie wszelki spam o charakterze pornograficznym również łamie polskie prawo. Przestępstwo to zagrożone jest niską karą i niestety w większości przypadków należy liczyć się z tym, że zostanie uznana „niska szkodliwość społeczna czynu"[38]. Szczególnym ograniczeniem jest zapis §2. przewidujący wyższą karę w przypadku prezentowania pornografii osobie, która nie

[33] J. Śpiewak, Wykorzystanie…, s. 33. Art. 200a dopisany został do listy katalogu przestępstw w przypadku których Policji wolno stosować techniki operacyjne. Interwencja ta może nastąpić, zanim dojdzie do spotkania z dzieckiem i jego skrzywdzenia.

[34] *Kodeks karny*…, art. 200b: „Kto publicznie propaguje lub pochwala zachowania o charakterze pedofilskim, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2".

[35] J. Śpiewak, Wykorzystanie…, s. 34.

[36] *Kodeks karny*…, art. 202: „Kto publicznie prezentuje treści pornograficzne w taki sposób, że może to narzucić ich odbiór osobie, która tego sobie nie życzy, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku (§1). Kto małoletniemu poniżej lat 15 prezentuje treści pornograficzne lub udostępnia mu przedmioty mające taki charakter albo rozpowszechnia treści pornograficzne w sposób umożliwiający takiemu małoletniemu zapoznanie się z nimi, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2" (§2).

[37] J. Śpiewak, Wykorzystanie…, s. 35.

[38] Tenże, *Aspekty*…, s. 1.

ukończyła 15 roku życia lub rozpowszechnianie pornografii bez skutecznego zabezpieczenia. Przepis ten jest niezwykle trudny w egzekwowaniu. Przeszkodą jest brak definicji „treści pornograficznych", „przedmiotów mających taki charakter" oraz konstrukcja przepisu. Wymaga on bowiem wskazania rzeczywistej osoby, które konkretnemu dziecku prezentowała czy udostępniła niewłaściwe materiały i udowodnienia tego faktu. W praktyce jest to na ogół niemożliwe. W przypadku serwisu internetowego wiąże się to z postawieniem przed sądem dziecka poniżej lat 15, które weszło na stronę www, przy czym ciężko stwierdzić, czy byłoby to już wystarczające do skazania twórcy lub administratora takiego serwisu, czy też konieczne byłoby jeszcze wykazanie, iż świadomie udostępnił on temu dziecku swoją stronę internetową[39]. Nasuwa się więc pytanie: czy zaproponowane rozwiązania są skuteczne?

Według jednego stanowiska wystarczy, że wydawca strony internetowej uprzedza o jej zawartości i wymaga, aby internauta, który chce przeglądać tę stronę miał ukończone 18 lat (z prawnego punktu widzenia wystarczy 15 lat). Jedyną formą weryfikacji wieku jest „kliknięcie" myszką i wybranie wariantu „wchodzę" lub „wychodzę". Stanowisko to zakłada, zupełnie złudnie, że każdy np. 14-latek spośród dwóch wariantów wybierze „wychodzę". Praktyka jest inna i w podobnym przykładzie znaczna część dzieci „klikając" na opcję „wchodzę", składa nieprawdziwe oświadczenie, co do swojego wieku. Nie sposób jest więc zgodzić się, że w powyższym przypadku obiektywnie, w sensie technicznym, uniemożliwiono małoletnim dostęp do treści pornograficznych. Wskazanie jednak efektywnego sposobu zapobiegania dostępowi dzieci do pornografii w Internecie rodzi szereg problemów. Wprowadzenie wymogu, aby użytkownik przesłał odpis dokumentu potwierdzającego jego wiek, wydaje się rozwiązaniem nazbyt restryktywnym. Trudno też wymóg ten zrealizować od strony technicznej. Pewnym rozwiązaniem, mogącym mieć zastosowanie jedynie w przypadku płatnych serwisów, jest obowiązek uiszczenia opłaty za pośrednictwem karty płatniczej. Jest to stosunkowo skuteczny, choć nie powszechny wśród wydawców stron pornograficznych sposób przeciwstawiania dostępowi małoletnich do zakazanych treści. Innym mankamentem jest praktyka właścicieli płatnych serwisów pornograficznych, którzy udostępniają za darmo pewną ilość zdjęć „próbnych", będących swoistą reklamą zachęcającą do skorzystania także z usług płatnych. Kolejnym ze sposobów zabezpieczających małoletnich przed stycznością z pornografią internetową jest zainstalowanie na komputerze, z którego korzysta dziecko, specjalnego oprogramowania filtrującego. Inną propozycją jest rozważenie przez UE możliwości wprowadzenia funkcjonalnej domeny głównej *(Generic Top Level Domaine)* zarezerwowanej dla stron stale kontrolowanych, których administratorzy zobowiązaliby się do poszanowania małoletnich i ich praw pod rygorem sankcji karnych (np. domena „KID")[40].

[39] Tenże, Wykorzystanie…, s. 35.

[40] R. Grabowski, *Wpływ internetu na ewolucję państwa i prawa*, Rzeszów 2008, s. 239–240.

4. Kierunki działania UE w zakresie stwarzania warunków dla rozwoju bezpiecznego Internetu

Główne kierunki działania UE w zakresie stwarzania warunków dla rozwoju bezpiecznego Internetu zostały zapisane w dokumencie *Safer Internet Action Plan, Work Programme 2003–2004*. Są to:

1. wspieranie inicjatyw budujących świadomość na temat bezpieczeństwa w Internecie – programy pomocowe (np. *Safer internet*);
2. promowanie umiejętności korzystania z Internetu;
3. tworzenie systemów filtracji i klasyfikacji treści dostępnych w globalnej sieci – techniczne urządzenia wspierające ochronę;
4. budowę bezpiecznej infrastruktury technicznej dostępu do Internetu[41].

Kierunki te zostaną teraz omówione z wyjątkiem czwartego, gdyż ten aspekt wykracza poza ramy tematyczne tej pracy.

ad 1. Wspieranie inicjatyw budujących świadomość na temat bezpieczeństwa w Internecie – programy pomocowe (np. *Safer internet*)

Wdrożenie priorytetów polityki ochrony dokonuje się poprzez realizację programów pomocowych Komisji Europejskiej. Jednym z nich jest *Safer Internet*[42], promujący bezpieczne korzystanie z sieci internetowej oraz nowych technologii *online* wśród dzieci i młodzieży. W ramach Programu prowadzone były również działania na rzecz zwalczania nielegalnych treści i spamu w globalnej sieci. Pierwotnie program przewidziany był na lata 1999–2002. Decyzją Rady został wydłużony o kolejne lata. Od 2005 roku do Programu włączona została problematyka związana z zagrożeniami wynikającymi z użytkowania gier sieciowych, wymianą plików P2P i innymi formami komunikacji *online* w czasie rzeczywistym (czaty i komunikatory). Bieżąca edycja obejmuje lata 2009–2013. Priorytetem *Programu* jest zwalczanie cyberprzemocy i uwodzenia dzieci w globalnej sieci[43].

Polskie Centrum programu *Bezpieczny Internet* powołane zostało w 2005 roku w ramach programu Komisji Europejskiej *Safer Internet*. Tworzą je Fundacja Dzieci Niczyje (dalej: FDN[44]) oraz Naukowa i Akademicka Sieć Komputerowa (dalej: NASK[45]) – koordynator. Centrum podejmuje szereg kompleksowych działań na rzecz bezpieczeństwa dzieci i młodzieży korzystających z Internetu

[41] *Dyzurnet.pl,* http://www.dyzurnet.pl/o_nas/historia.html (odczyt z dn. 9 maja 2011 r.).

[42] *Safer Internet,* http://ec.europa.eu/information_society/activities/sip/index_en.htm (odczyt z dn. 4 maja 2011 r.).

[43] Safer Internet Programme: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/index_en.htm (odczyt z dn. 7 maja 2011 r.).

[44] Więcej informacji: *Fundacja Dzieci Niczyje,* www.fdn.pl (odczyt z dn. 27 maja 2011 r.).

[45] Więcej informacji: *Naukowa i Akademicka Sieć Komputerowa,* www.nask.pl (odczyt z dn. 8 maja 2011 r.).

i nowych technologii. Partnerem projektów realizowanych przez Centrum jest Fundacja Orange. Ciałem doradczym jest Komitet Konsultacyjny. Współpraca Centrum z instytucjami rządowymi, pozarządowymi, placówkami oświatowymi oraz podmiotami komercyjnymi realizowana jest w ramach Ogólnopolskiej Koalicji na rzecz Bezpieczeństwa w Internecie, stanowiącej platformę dystrybucji informacji o różnych inicjatywach chroniących dzieci[46]. Ochronie małoletnich służy Centrum Monitoringu Sieci Internet, utworzone wspólnie przez NASK oraz fundację Kidprotect.pl. Każdy użytkownik Internetu może zgłaszać pocztą elektroniczną, telefonicznie, faksem lub wykorzystując formularze ze stron www[47] wszelkie tematy sieciowej pornografii i pedofilii dziecięcej. Przekazane informacje są weryfikowane, po czym jeżeli zachodzi uzasadnione podejrzenie popełnienia przestępstwa następuje zawiadomienie organów ścigania (Policji, prokuratury) i przekazanie im zgromadzonych w sprawie materiałów. Kolejną inicjatywą NASK jest ogólnopolska kampania *Kawiarenka Przyjazna Dzieciom*. Akcja, zapoczątkowana w grudniu 2008 r., ma na celu zwrócenie uwagi właścicieli kawiarenek internetowych na bezpieczeństwo korzystających z jej usług dzieci. Doświadczenie i wiedza NASK stanowią podstawę utworzenia zespołu kontaktowego Dyżurnet.pl.

Drugim realizatorem programu *Safer Internet* jest FDN. Jest to organizacja pozarządowa o charakterze non-profit, która od 1991 roku zajmuje się szeroko rozumianą pomocą dzieciom krzywdzonym, ich rodzinom i opiekunom. Od 2004 roku Fundacja prowadzi ogólnopolską kampanię społeczną na rzecz bezpieczeństwa najmłodszych internautów *Dziecko w sieci*. Ponadto jest zaangażowana w wiele projektów międzynarodowych. Od 2005 roku jest narodowym koordynatorem projektu *Awareness,* realizowanego we współpracy z NASK. Od lutego 2007 r. FDN we współpracy z Fundacją Orange prowadzi helpline.org.pl – punkt pomocowy dla dzieci. Fundacja jest także członkiem „Dynamicznej Koalicji na rzecz Bezpieczeństwa Dzieci w Internecie"[48], powołanej podczas *II Forum Zarządzania Internetem* w 2007 roku.

Prowadzone od 1 stycznia 2005 r. projekty: *Awareness* – realizowany przez Konsorcjum NASK i FDN oraz projekt *Dyżurnet* prowadzony przez NASK, obecnie ujęte zostały w jeden wspólny projekt *Saferinternet.pl*[49]. Celem tego projektu jest zwiększanie społecznej świadomości na temat zagrożeń, jakie niosą ze sobą najnowsze techniki komunikacji. Wśród podejmowanych działań priorytetem jest edukacja (dzieci i rodziców), a także podnoszenie kompetencji

[46] *Safer Internet w Polsce,* http://www.saferinternet.pl/safer_internet_w_polsce.html (odczyt z dn. 7 maja 2011 r.).

[47] *Computer Emergency Response Team*, www.cert.pl (odczyt z dn. 9 maja 2011 r.); *Fundacja Kidprotect.pl,* www.kidprotect.pl (odczyt z dn. 9 maja 2011 r.).

[48] *Dynamiczna Koalicja na rzecz Bezpieczeństwa Dzieci w Internecie,* http://www.dzieckowsieci.pl/strona.php?p=116 (odczyt z dn. 9 maja 2011 r.).

[49] Więcej informacji: *Saferinternet.pl*, www.saferinternet.pl (odczyt z dn. 10 maja 2011 r.); *Projekt Saferinternet.pl,* http://www.dzieckowsieci.pl/strona.php?p=75 (odczyt z dn. 10 maja 2011 r.).

profesjonalistów w zakresie bezpiecznego korzystania z internetu. W ramach *Saferinternet.pl* działa: zespół Dyżurnet.pl (tzw. *hotline*) – narodowy punkt kontaktowy do zwalczania nielegalnych treści w internecie oraz zespół Helpline.org.pl – punkt pomocowy dla osób, które doświadczyły przemocy w świecie online.

Zespół Dyżurnet.pl powstał w 2006 roku przy NASK w ramach programu *Safer Internet Action Plan*[50]. Współpraca narodowych zespołów *hotline* następuje w ramach stowarzyszenia INHOPE (*The Association of Internet Hotline Providers*). Projekt utworzenia *hotline'u* powstał w odpowiedzi na inicjatywę KE tworzenia takich punktów kontaktowych wyrażoną w formie *Call for Proposals 2003/2004*[51].

Dyżurnet.pl jest punktem, do którego można anonimowo zgłaszać przypadki występowania w internecie treści zabronionych prawem[52]. W latach 2005–2009 najwięcej (ponad 1/3) zgłoszeń dotyczyło pornografii dziecięcej, kolejno „inne treści" (19%) oraz pornografii dorosłych (18%). Uwagę zwraca wzrost liczby zgłoszeń klasyfikowanych jako „inne treści"[53] z kilku (w roku 2005 – 4%) do kilkunastu procent (w roku 2009 – 19%). W zależności od lokalizacji serwera (w Polsce lub poza jej granicami) informacje o treściach nielegalnych są przekazywane do Komendy Głównej Policji lub do innych punktów kontaktowych zrzeszonych w stowarzyszeniu INHOPE. Wobec treści legalnych, ale potencjalnie szkodliwych dla dzieci, znajdujących się na polskich serwerach, podejmowane są działania zmierzające do szybkiego ich usunięcia. Zespół Dyżurnet.pl włącza się w realizowane przez Europol oraz *Child Exploitation and Online Protection Centre* projekty – europejskiej platformy wymiany informacji o zagrożeniach w internecie oraz Koalicji Finansowej, której celem jest zwalczanie dystrybucji pornografii dziecięcej w globalnej sieci[54].

Ważną rolą Zespołu jest podnoszenie świadomości użytkowników internetu. W ramach edukacyjnych przedsięwzięć w latach 2005–2009 przeprowadzono cykl 18 lokalnych konferencji wojewódzkich dedykowanych dla nauczycieli, pedagogów, przedstawicieli władz samorządowych i organizacji pozarządowych, policji, dostawców usług internetowych (przeszkolonych zostało łącznie 1600 osób). Dyżurnet.pl przy udziale zespołu CERT Polska przeprowadził dwie edycje testów skuteczności blokowania programów filtrujących. Ich wyniki zostały

[50] Więcej informacji: Zespół Dyżurnet.pl, www.dyzurnet.pl (odczyt z dn. 27 maja 2011 r.).

[51] *Historia Dyzurnet.pl,* http://www.dyzurnet.pl/o_nas/historia.html (odczyt z dn. 9 maja 2011 r.).

[52] Zgłoszenia można kierować przez formularz kontaktowy znajdujący się na stronie www.dyzurnet.pl, na adres mailowy dyzurnet@dyzurnet.pl lub poprzez infolinię 801 615 005.

[53] To materiały brutalne, makabryczne, obsceniczne (zdjęcia ofiar wypadków, kanibalizm, deformacje ciała, bestialstwo wobec zwierząt). Zgłoszenia dotyczą propagowania niebezpiecznych zachowań (nakłanianie do aborcji (dokonywanej domowymi sposobami), propagowania działalności sekt, namawiania do samookaleczeń, samobójstw, stosowania używek i innych substancji psychoaktywnych, promowania bulimii i anoreksji.

[54] Dyżurnet.pl. *Raport z działalności zespołu w latach 2005–2009*, Warszawa 2010, s.11. Raport dostępny na stronie: http://www.dyzurnet.pl/images/stories/PDF/dyzurnet_raport_5lat.pdf

opisane w raportach *Jak skutecznie filtrować zawartość internetu?* (2007)[55] oraz *Rozwiązania filtrujące niepożądane treści w internecie* (2009)[56]. Jedną z ostatnich inicjatyw zespołu Dyżurnet.pl było opublikowanie scenariuszy zajęć *Jak w necie? Bezpiecznie!*[57], przeznaczonych dla nauczycieli klas gimnazjalnych. Wspólną inicjatywą NASK oraz FDN jest organizowana od 2007 roku Międzynarodowa Konferencja w Warszawie: *Bezpieczeństwo dzieci i młodzieży w internecie*[58]. Każdego roku organizatorzy próbują zwrócić szczególną uwagę na inne aspekty ochrony[59].W najbliższym okresie Dyżurnet.pl zamierza skupić swoją działalność wokół następujących zagadnień: rozwinięcie współpracy z sygnatariuszami *Ogólnopolskiej Koalicji na rzecz Bezpieczeństwa w Internecie*; szerzenie idei Bezpiecznego Internetu w państwach środkowowschodniej Europy; wypracowanie platformy współpracy z grupą dostawców usług internetowych; współudział w budowie europejskiej platformy wymiany informacji o zagrożeniach w globalnej sieci; udział w procesie szkolenia sędziów i prokuratorów w Krajowej Szkole Sądownictwa i Prokuratury oraz współpraca z Polską Radą Ekumeniczną[60].

Drugi Zespół: Helpline.org.pl to wspólny projekt FDN i Fundacji Orange w ramach programu *Safer Internet*. Został uruchomiony 6 lutego 2007 r. w *Dniu Bezpiecznego Internetu*. Celem projektu jest pomoc młodym internautom, rodzicom i profesjonalistom w przypadkach zagrożeń związanych z korzystaniem z internetu, a także inicjowanie zmian systemowych, które pozwolą skuteczniej chronić najmłodszych użytkowników nowych technologii[61].

Obecnie we wszystkich krajach Unii Europejskiej działają podobne projekty, wspierające bezpieczeństwo w internecie oraz podnoszenie kompetencji medialnych. Noszą różne nazwy (np. klicksafe.de – niemiecki partner programu *Safer Internet*), ich priorytety są zależne od realiów danego kraju. Ściśle jednak ze sobą współpracują, dzięki czemu wśród państw zjednoczonej Europy zapewniona jest wymiana informacji i najlepszych rozwiązań. Wszystkie projekty krajowe należą do sieci INSAFE (*Internet Safety Awareness for Europe*).

Współdziałanie zespołów Helpline.org.pl oraz Dyżurnet.pl w ramach Saferinternet.pl, pozwala na realizowanie idei, które zwiększają bezpieczeństwo dzieci

---

[55] I. Jończyk, M. Różycka, K. Kurowski, A. Węgłowski, *Jak w necie? Bezpiecznie!,* Warszawa 2007.

[56] *Rozwiązania filtrujące niepożądane treści w internecie*. Raport Dyżurnet.pl, Warszawa 2009.

[57] *J@k w necie? Bezpiecznie!!! Warsztaty dla klas gimnazjalnych,* Warszawa 2009.

[58] Międzynarodowa Konferencja: Bezpieczeństwo dzieci i młodzieży w internecie, http://konferencja.saferinternet.pl/artykuly-2010/iv_miedzynarodowa_konferencja_bezpieczenstwo_dzieci_i_ mlodziezy_w_internecie.html (odczyt z dn. 11 maja 2011 r.).

[59] Ogólne zagadnienia dotyczące bezpieczeństwa dzieci w internecie (2007); aspekty prawne, a także rola Policji i współpracy międzynarodowej w opracowywaniu i udoskonalaniu sposobów ochrony najmłodszych (2008); blokowanie na poziomie operatorskim treści pornograficznych z udziałem dzieci (2009); bezpieczeństwo w serwisach społecznościowych oraz zagadnienia ochrony prywatności (2010).

[60] Dyżurnet.pl. *Raport*…, s. 22.

[61] Helpline.org.pl, http://www.dzieckowsieci.pl/strona.php?p=101 (odczyt z dn. 11 maja 2011 r.).

i młodzieży w internecie. Szeroki krąg odbiorców (dzieci, nauczyciele, policjanci, sędziowie i prokuratorzy, a także przedstawiciele instytucji rządowych oraz firm związanych z internetem) wymaga różnorodnych działań. Przedstawiciele tych Zespołów włączają się w dyskusje, uczestniczą, a także organizują konferencje i szkolenia oraz na co dzień odpowiadają na zgłoszenia internautów. Współpraca na poziomie międzynarodowym (INSAFE, INHOPE) pozwala na prowadzenie wspólnych działań z podobnymi organizacjami europejskimi i światowymi.

Zarówno Dyżurnet.pl, jak i Helpline.org.pl realizują założenia Komisji Europejskiej. W ramach projektu *Safer Internet,* dzięki wielu płaszczyznom współpracy, realizowane są różne inicjatywy międzynarodowe na rzecz zwiększenia bezpieczeństwa dzieci. Są to: obchody *Dnia Bezpiecznego Internetu;* krajowe projekty *Safer Internet*; *Forum Safer Internet*; działanie stowarzyszenia INHOPE; spotkania o zasięgu międzynarodowym regionalnych zespołów reagujących (*hotline'y, helpline'y*, Policja) z przedstawicielami rządowymi; Koalicja Finansowa na rzecz zwalczania dystrybucji pornografii dziecięcej oraz Europejska platforma wymiany informacji o zagrożeniach w internecie[62].

W ramach programu *Safer Internet*, NASK oraz FDN do końca 2010 r. zrealizowały następujące projekty:

- uruchomiono *Helpline* – punkt pomocowy: www.helpline.org.pl;
- przeprowadzono badania dotyczące stanu bezpieczeństwa w kawiarenkach internetowych;
- przeprowadzono testy programów filtrujących;
- zorganizowano promocję zespołu Dyżurnet.pl – punkt kontaktowy: www.dyzurnet.pl;
- przeprowadzono kampanię społeczną *Dziecko w sieci*;
- zorganizowano 4 Międzynarodowe Konferencje *Bezpieczeństwo dzieci i młodzieży w* internecie oraz18 wojewódzkich konferencji *Bezpieczny Internet*;
- zorganizowano kolejne obchody *Dnia Bezpiecznego Internetu*;
- powołano *Ogólnopolską Koalicję na rzecz Bezpieczeństwa w Internecie*;
- uruchomiono serwisy internetowe: *Safer Internet w Polsce:* www.saferinternet.pl; *Dziecko w sieci:* www.dzieckowsieci.pl; *Dzień Bezpiecznego Internetu:* www.dbi.pl;
- zorganizowano serwisy edukacyjne dla dzieci: *Sieciaki:* www.sieciaki.pl; *Sieciaki Przedszkolaki*: www.przedszkolaki.sieciaki.pl.
- To tylko wybrane działania zrealizowane w ramach projektu *Saferinternet.pl* w Polsce.

ad. 2. Promowanie umiejętności korzystania z Internetu

Kolejną formą ochrony użytkowników Internetu jest edukacja medialna. Web 2.0, idea internetu, w którym głównymi twórcami treści są sami internauci, stawia nowe wyzwania przed edukacją medialną. Dotychczasowe kompetencje

[62] *Dyżurnet.pl. Raport…*, s.11.

medialne, związane z umiejętnością krytycznego odbioru mediów zostają poszerzone o kolejny wymiar – amatorską twórczość. Koresponduje to z koncepcją kultury uczestnictwa[63], w której jest ona spostrzegana jako pochodna aktywności obywatelskiej, a twórczość – jako element życia społecznego. Równocześnie stwarza nowe problemy – współczesna edukacja jest bowiem wciąż rozdarta pomiędzy „paradygmatem Columbine" (ochroną dzieci przed zagrożeniami związanymi z wykorzystaniem nowych mediów), a „paradygmatem pokolenia sieci" (w myśl którego wystarczy posadzić młodych ludzi przy komputerach, by wykorzystali je do spontanicznej twórczości i poszerzania swojej wiedzy)[64].

Komisja Europejska nie posiada kompetencji w krajowych systemach oświaty, stąd nie może nałożyć na państwa członkowskie UE obowiązku wprowadzenia edukacji medialnej jako odrębnego przedmiotu nauczania w szkołach. Zadaniem, jakie stawia sobie Komisja, jest wywołanie powszechnej debaty na temat bezpiecznego korzystania z internetu i innych mediów. Nasuwa się pytanie: czym jest umiejętność korzystania z internetu? kto przede wszystkim jest odpowiedzialny za edukację medialną dzieci?

W myśl *Dyrektywy Parlamentu Europejskiego i Rady o audiowizualnych usługach medialnych z 2010 r*. na umiejętność korzystania z Internetu składają się:

- sprawność, wiedza i osąd, które pozwalają konsumentom skutecznie i bezpiecznie używać mediów;
- świadome wybory odbiorców, którzy zdają sobie sprawę z charakteru treści i usług;
- korzystanie z całego zakresu nowych technologii komunikacyjnych;
- ochrona odbiorcy i jego rodziny przed materiałami szkodliwymi lub obraźliwymi[65].

Zgodnie z Zaleceniami Komisji Europejskiej z 2007 i 2009 roku: *Europejskie podejście do umiejętności korzystania z mediów w środowisku cyfrowym*, umiejętność ta to: „zdolność do korzystania z mediów, rozumienia, krytycznej oceny różnych aspektów mediów i ich treści oraz porozumiewania się w różnych kontekstach. Obejmuje wszystkie media, w tym internet i wszelkie inne technologie cyfrowe"[66]. Zalecenia podkreślają kilka aspektów tejże umiejętności. Po pierwsze,

---

[63] H. Jenkins, *Kultura konwergencji. Zderzenie starych i nowych mediów*, Warszawa 2007.

[64] M. Filiciak, *Nowe wyzwania edukacji medialnej: Web 2.0. Materiały konferencyjne z III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie; Warszawa 29–30 września 2009 r.,* Warszawa 2009, s. 26.

[65] *Dyrektywa 2010/13/UE Parlamentu Europejskiego i Rady z dnia 11 marca 2010 r. o audiowizualnych usługach medialnych,* zmieniająca dyrektywę Rady 89/552/EWG w sprawie koordynacji niektórych przepisów ustawowych, wykonawczych i administracyjnych Państw Członkowskich, dotyczących wykonywania telewizyjnej działalności transmisyjnej, Dz.U. L 332 z 18 grudnia 2007.

[66] *Zalecenie Komisji COM(2009)6464 z dnia 20 sierpnia 2009 r. w sprawie umiejętności korzystania z mediów w środowisku cyfrowym w celu stworzenia bardziej konkurencyjnego sektora audiowizualnego i treści cyfrowych oraz stworzenia integracyjnego społeczeństwa opartego na wiedzy*, Dz.U. L 227 z 29.8.2009.

wyposażenie użytkowników w odpowiednie narzędzia służące do krytycznej oceny treści online. Po drugie, rozszerzenie kreatywności i umiejętności produkcyjnych oraz zwiększenie świadomości w odniesieniu do praw autorskich. Po trzecie, zapewnienie, że każdy może odnosić korzyści ze społeczeństwa informacyjnego, w tym osoby w niekorzystnej sytuacji z uwagi na ograniczone zasoby albo wykształcenie, wiek, płeć, pochodzenie etniczne, niepełnosprawność (e-Dostępność) oraz osoby żyjące na obszarach mniej uprzywilejowanych (wszystkie te kwestie objęte są programem e-Integracja). Po czwarte, podnoszenie świadomości w zakresie funkcjonowania wyszukiwarek (priorytetyzacja odpowiedzi) i innych technologii filtrujących.

Komisja proponuje różne poziomy odbioru mediów. Są to:

- łatwość korzystania ze wszystkich mediów, od gazet drukowanych po internet;
- aktywne korzystanie z mediów poprzez interaktywną telewizję, używanie wyszukiwarek internetowych, udział w społecznościach wirtualnych, lepsze wykorzystywanie potencjału mediów (np. poprzez korzystanie z bibliotek wirtualnych);
- krytyczne podejście do mediów odnośnie ich jakości i treści;
- kreatywne używanie mediów;
- rozumienie ekonomii mediów oraz różnicy między pluralizmem a własnością mediów;
- świadomość w zakresie zagadnień związanych z prawami autorskimi, które są niezbędne dla kultury legalności, w szczególności dla młodszej generacji występującej zarówno jako konsumenci jak i producenci treści[67].

Ponadto Komisja Europejska zaproponowała szereg działań mogących kształtować umiejętność korzystania z globalnej sieci. W szczególności:

- stałe szkolenie nauczycieli, we współpracy ze stowarzyszeniami ochrony dzieci, w zakresie pedagogicznych metod bezpiecznego korzystania;
- wprowadzenie specjalnego nauczania w zakresie internetu skierowanego do dzieci;
- zajęcia otwarte dla rodziców;
- organizowanie krajowych kampanii informacyjnych skierowanych do obywateli, w celu ostrzeżenia opinii publicznej przed niebezpieczeństwami związanymi z internetem i przed ryzykiem sankcji karnych (informacje o możliwościach wnoszenia skarg lub stosowania kontroli rodzicielskiej). Specjalne kampanie można skierować do określonych grup docelowych (np. do rodziców);
- dystrybucję materiałów informacyjnych na temat ryzyka związanego z internetem *(jak bezpiecznie korzystać z sieci)* oraz korzystania z infolinii przeznaczonych do przyjmowania skarg;
- zakładanie lub poprawę skuteczności działających gorących linii telefonicznych, dla ułatwienia składania skarg i zgłaszania istnienia szkodliwych stron internetowych[68].

[67] *Tamże*, s. 4.

[68] *Tamże*.

Przykładowe działania i inicjatywy w tym zakresie to:

- program pomocowy Unii Europejskiej *Safer Internet* mający na celu wyposażenie internautów w narzędzia do krytycznej oceny treści online;
- kampanie społeczne: *Dzień Bezpiecznego Internetu*;
- spoty telewizyjne: *Gdzie jest Klaus?* (Niemcy), *Nigdy nie wiadomo, kto jest po drugiej stronie ekranu* (Polska), *Pomyśl, zanim wyślesz (UE);*
- gry internetowe: *Przez dzikie internetowe lasy* – opracowana w 6 językach;
- serwisy internetowe dla dzieci: Sieciaki.pl;
- poradniki i podręczniki, np: *eSafety* zawierający historyjki i ćwiczenia dla dzieci – opublikowany w 10 językach.

Dlaczego edukacja na temat mediów, funkcjonowania internetu powinna rozpocząć się w rodzinie? W tym wieku – jak wynika z badań Lucyny Kirwil:

- kształtuje się u dzieci wizja świata w kategoriach „przyjazny – zagrażający – wrogi";
- ocena realizmu świata przedstawionego w mediach dokonana przez dziecko wyznacza, w jakim zakresie dziecko będzie przejmować wzorce prezentowane w mediach;
- dzieci mają ukształtowaną rozwojową gotowość do uczenia się wszystkich rodzajów treści, będą więc w stanie efektywnie korzystać z podstaw edukacji medialnej.

Należy także wyróżnić dwa wymiary tejże edukacji w rodzinie: edukację medialną rodziców i opiekunów oraz edukację dzieci i innych domowników prowadzoną przez rodziców. „Rodzicom – jak stwierdziła Kirwil – konieczna jest edukacja medialna ze względu na ich lękowy lub bezkrytyczny stosunek do mediów".

ad 3. Tworzenie systemów filtracji i klasyfikacji treści dostępnych w globalnej sieci – techniczne urządzenia wspierające ochronę

Prawna kontrola przepływu informacji w globalnej sieci budzi kontrowersje o charakterze filozoficznym i politycznym. W celu ochrony użytkowników internetu (np. ochrony danych osobowych, prywatności) opracowywane są standardy techniczne wspomagające ochronę. Technika stwarza możliwość ochrony określonych grup internautów przed negatywnym wpływem materiałów dostępnych w internecie bez naruszenia wolności słowa innych ludzi. Stanowi to alternatywę w stosunku do rozwiązań prawnych.

Zalecenia stosowania technologii wspomagających ochronę najmłodszych internautów zawiera program Unii Europejskiej *Safer Internet Plus. Program* deklaruje finansowanie:

- działań informacyjnych na temat filtrującego oprogramowania;
- projektów mających na celu dostosowanie systemów klasyfikacji i znaków jakości do konwergencji usług telekomunikacyjnych i technologii informacyjnej;
- zachęcenie dostawców treści do uczestnictwa w systemach klasyfikacji treści i ubiegania się o znaki jakości;

- badań wpływu nowych technologii na dzieci już na etapie ich opracowywania, a nie zwalczanie każdego skutku tych technologii po tym, jak zostały już opracowane;
- środków technicznych, umożliwiających użytkownikom ograniczanie ilości niechcianych i szkodliwych treści oraz zarządzanie niechcianą korespondencją;
- dostępności technologii filtrujących, zwłaszcza w przypadku języków narodowych niewystarczająco popularnych na rynku internetowym;
- wspieranie środków technologicznych zwiększających prywatność[69].

Obecnie dostępnych jest kilka narzędzi technicznych umożliwiających zapobieganie zagrożeniom związanym z używaniem internetu przez dzieci i młodzież. Są to oprogramowania:

- filtrujące strony internetowe;
- służące do monitoringu i kontroli treści internetowych;
- służące do weryfikacji wieku internauty;
- oraz inne narzędzia techniczne wspierające ochronę[70].

Poniżej krótka charakterystyka.

Oprogramowanie filtrujące

Oprogramowanie filtrujące umożliwia selekcjonowanie i wyodrębnianie treści internetowych. W kontekście ochrony użytkowników internetu może chronić ono dzieci przed przypadkowym lub zamierzonym kontaktem ze szkodliwymi, niezgodnymi z prawem lub nieodpowiednimi treściami. Należy jednak pamiętać, że dzieci i młodzież posiadają dużą wiedzę informatyczną, a działanie wielu filtrów można w prosty sposób obejść. Działanie programów filtrujących oparte jest na listach zakazanych treści lub analizie stron internetowych metodami semantycznymi oraz statystycznymi. Mogą one działać jako odrębna aplikacja lub moduł oprogramowania użytkownika końcowego w punktach centralnych dostępu do internetu (np. na serwerach proxy) lub na poziomie providera internetowego. Treści mogą być filtrowane za pomocą arbitralnej klasyfikacji (na zasadzie „czarnych" i „białych" list), klasyfikacji automatycznej (na zasadzie blokowania słów kluczowych), a także na podstawie oceny treści, weryfikowanej przez niezależną agencję (np. Netherlands Institute for the Classifikation of Audiovisual Media jako administratora systemu PEGI) lub przez samego dostawcę treści (np. *Internet Content Rating Association*[71]). Większość programów filtrujących łączy w sobie różne metody klasyfikacji treści. Działanie systemu uzależnione jest od używanej przeglądarki. Jeżeli ta wspiera standard PICS (np. Internet

[69] *Safer Internet Plus, o*publikowano w Dz. Urz. C 208 E/48 z 25.8.2005.

[70] Stiftung Digitale Chancen, *dz. cyt*., s. 7.

[71] Więcej na temat klasyfikacji ICRA: www.fosi.org/cms/ (odczyt z dn. 27lipca 2009)].

Explorer), po pobraniu dokumentu HTML następuje odczytanie i interpretacja dołączonego do niego kodu PICS. Na podstawie zawartych tam informacji przeglądarka podejmuje decyzję o wyświetleniu lub odmowie wyświetlenia strony. Rodzice lub inni opiekunowie, za pomocą tego systemu i bazujących na nim programów, takich jak np. *DansGuardian, Net Nanny, CyberPatrol, Surw Watch,* mogą ustanawiać reguły korzystania z zasobów internetu przez pozostających pod ich opieką dzieci. Oprogramowanie filtrujące uważane jest za narzędzie, które pozwala na rozwiązanie wielu problemów. Jest jednak mniej skuteczne w przypadku treści i zachowań, które trudno precyzyjnie scharakteryzować. Obecnie brakuje regulacji w zakresie międzynarodowych oznaczeń, które informowałyby o przeznaczeniu zamieszczonych treści dla danej kategorii wiekowej[72].

Monitoring i kontrola

Monitoring oznacza automatyczne badanie lub sprawdzanie systemów i usług za pomocą mechanizmu filtrującego, którego wyniki – w celu uzyskania lepszych i bardziej miarodajnych rezultatów – są następnie poddawane ocenie ekspertów, decydującego czy treści mają zostać przefiltrowane, czy usunięte. Zazwyczaj proces weryfikacji przeprowadzany jest na podstawie losowej próbki skanowanych treści. System monitoringu pozwala np. na sprawdzenie zapisów sesji czatu, wpisów na blogach czy też zamieszczanych lub wymienianych zdjęć.

Stosowanie monitoringu i kontroli umożliwia w pewnym stopniu weryfikowanie treści internetowych oraz komunikacji przez internet. Może się to odbywać na różnych etapach procesu przechowywania i udostępniania treści. Ogólnie monitoring i ochrona są bardziej skuteczne niż samo oprogramowanie filtrujące. Dzieje się tak, ponieważ w przypadku monitoringu, decyzja o usunięciu treści internetowych lub blokowaniu aktywności w globalnej sieci podejmowana jest na podstawie oceny dokonanej przez specjalistę. Są najskuteczniejszym narzędziem w przypadku treści nieodpowiednich dla dzieci. Wykrywalność na poziomie 2/5 treści zawierających przemoc, treści niezgodnych z prawem, a także treści zachęcających do samookaleczenia pozwala stwierdzić, że skuteczność tego narzędzia w odniesieniu do zagrożeń tego typu jest tylko nieznacznie niższa. Szacuje się, że monitoring i kontrola umożliwiają wykrycie co najmniej 1/3 przypadków szkodliwych porad, prześladowań, nieodpowiednich dla dzieci reklam, *groomingu,* kradzieży tożsamości. Mogą wykryć 1/4 ataków *phishingu* oraz zapobiec uzależnieniu od internetu, tylko w jednym na sześć przypadków[73].

[72] *Rozwiązania filtrujące niepożądane treści w internecie. Raport Dyżurnet.pl*, Warszawa 2009, s. 4.

[73] *Tamże,* s. 20–21.

Weryfikacja wieku

Do weryfikacji wieku internautów oraz uzyskania gwarancji, że określonym grupom wiekowym dostarczane są jedynie odpowiednie dla nich usługi i treści, stosowane są różne systemy. Weryfikacja wieku może odbywać się poza internetem, na podstawie jednorazowego kontaktu osobistego. Oznacza to, że po identyfikacji i weryfikacji wieku, użytkownik uzyskuje dane pozwalające mu na dostęp do serwisu – hasło lub PIN. Takie zabezpieczenie stosowane jest zazwyczaj w przypadku usług płatnych, przy czym to ich właściciel (ryzykując utratę pieniędzy) powinien zadbać, by nie zostały one użyte w niewłaściwy sposób. Zaawansowane systemy identyfikacji i weryfikacji wieku opierają się na koncepcji jednoczesnego użycia określonego urządzenia oraz określonej wiedzy (PIN lub hasła). Tylko osoba, która jednocześnie dysponuje i urządzeniem, i wiedzą może udowodnić, że jest prawnym właścicielem tożsamości, a zatem – że należy do określonej grupy wiekowej. Ten rodzaj technicznej weryfikacji wieku zapewnia wyższą skuteczność, wymaga jednak specjalnego sprzętu (np. czytnika kart), a także istnienia odpowiednich uregulowań prawnych.

Obecnie prawodawstwo wielu państw europejskich umożliwia weryfikację wieku w celu ograniczenia dostępu dzieci do treści przeznaczonych dla dorosłych. Istnieje kilka systemów weryfikacji przeznaczonych dla małoletnich (takich jak np. dziecięca karta w Belgii), które pozwalają za pomocą środków technicznych na zagwarantowanie dzieciom i młodzieży bezpiecznego dostępu do specjalnych obszarów w internecie (np. dziecięcych pokojów czatowych). Jednym z pierwszych państw stosujących systemy weryfikujące wiek internauty są Niemcy. Rozwinęły się różne systemy i techniki weryfikacji użytkownika internetu: należy zalogować się na wybranej stronie, następnie wysłać kopię dowodu osobistego lub karty kredytowej do ISP; logowanie poprzedzone może być też podpisaniem w świecie realnym umowy z dostawcą dostępu do internetu (jest to pretekst do spotkania, by móc sprawdzić wiek potencjalnego internauty). Najważniejsze systemy weryfikujące wiek użytkownika internetu to: ARCOR, Blue Movie/Erotic Media i inne.

Weryfikacja wieku odgrywa istotną rolę przy ograniczeniu dostępu małoletnich do określonych treści lub serwisów umożliwiających nawiązanie kontaktów z dorosłymi. Cechuje się wyższą skutecznością w przypadku treści nieodpowiednich dla określonych grup wiekowych (w niemal połowie przypadków) i treści zawierających przemoc niż w przypadku pozostałych zagrożeń. Może doprowadzić do wykrycia od 1/4 do 1/5 przypadków treści niezgodnych z prawem oraz reklamę nieodpowiednią dla dzieci. Może zapobiec jednemu na siedem aktów *groomingu*. Technologia ta nie pozwala na skuteczne zapobieganie zachęcaniu do samookaleczenia. Wykazuje niską skuteczność w przypadku takich zagrożeń jak szkodliwe porady, a w przypadku wszystkich pozostałych zagrożeń uważana jest za praktycznie nieskuteczną[74].

[74] Stiftung Digitale Chancen, *dz. cyt*., s. 21–22.

Inne narzędzia techniczne wspomagające ochronę

Obok oprogramowania służącego do weryfikacji wieku internauty stosowanych jest jeszcze kilka innych narzędzi technicznych wspomagających ochronę dzieci. Między innymi:

Kontrola czasu, jak wskazuje nazwa, może być używana do ograniczania czasu korzystania z komputera, (po upływie zaplanowanego czasu korzystania z sieci, następuje automatyczne wyłączenie urządzenia). Eksperci oceniają, że metoda ta może zapobiec co drugiemu przypadkowi uzależnienia od internetu.

Procesy automatycznego uwierzytelniania opierają się na przedmiotach, które dana osoba posiada (np. karcie identyfikacyjnej, dowodzie osobistym), jej wiedzy (PIN lub hasło) oraz cechach danej osoby (np. fizycznych – odcisku palca). Są często oparte na kryptografii asymetrycznej, jak np. podpis cyfrowy. Zdaniem ekspertów metoda ta może zapobiec ponad 1/3 przypadków kradzieży tożsamości.

Tzw. mechanizm *anty-groomingowy* jest rozwiązaniem, które łączy w sobie kilka metod pozwalających na wykrycie zachowań odbiegających od normy i zapobiec w ten sposób próbom uwodzenia małoletnich w pokojach czatowych. Mechanizm opiera się na bazie zawierającej profile typowych zachowań osób próbujących uwodzić dzieci w świecie rzeczywistym oraz realnych dzieci. Profile te są budowane na podstawie analizy słownictwa, długości zdań, interpunkcji, tempa pisania i poziomu agresji. Są one regularnie aktualizowane, dzięki czemu mechanizm może odróżnić pozytywne kontakty od tych negatywnych, grożących nadużyciem lub przestępstwem. Jeżeli istnieją przesłanki pozwalające uznać daną znajomość za niewłaściwą, za pomocą SMS-a, e-maila lub panelu kontrolnego na komputerze opiekuna, kierowane jest do niego powiadomienie. Skuteczność mechanizmu ocenia się na porównywalnym poziomie jak monitoring i kontrola (ok. 2/5 przypadków)[75].

Czy powyższe rozwiązania techniczne zapewniają ochronę dzieciom? Na podstawie testów przeprowadzonych przez NASK[76] oraz informacji zawartych na stronach producentów oprogramowania filtrującego nasuwają się następujące wnioski:

- programy filtrujące dość skutecznie blokują dostęp do stron zawierających pornografię lub erotykę; w przypadku stron pornograficznych innych niż polskojęzyczne i anglojęzyczne, filtry nie spełniają swej funkcji;
- pozwalają na wyświetlenie stron zawierających treści o charakterze rasistowskim, propagujących używki, leki czy ryzykowne zachowania;
- programy mają trudności ze skutecznym filtrowaniem stron zawierających wyłącznie grafikę;
- niektóre filtry zbyt wolno analizują strony i pozwalają na ich wyświetlenie;
- w przypadku treści obojętnych/nieszkodliwych aplikacje błędnie reagują na pewne słowa kluczowe (seks, piersi, kotki), powodując zablokowanie strony;

[75] *Tamże*, s. 22–24.

[76] *Rozwiązania filtrujące niepożądane…*, s. 8–34.

- mimo zapewnień producentów programy pozwalają na wysyłanie danych osobowych, korzystanie z komunikatorów, list dyskusyjnych, czatów oraz poczty elektronicznej;
- w niedostateczny sposób rozpoznają zawartość Web 2.0 – serwisów społecznościowych, blogów oraz portali, na których udostępnia się pliki muzyczne oraz filmowe;
- większość programów nie kontroluje korzystania z gier zainstalowanych na komputerze lub dostępnych online; niektóre pozwalają na dostęp do gier ewidentnie erotycznych;
- w przypadku używania krótkiego adresu URL lub bramki *proxy* aplikacje słabo rozpoznają treści niepożądane (sposób na obejście blokad rodzicielskich);
- alert blokady nie zawsze informuje o powodzie zamknięcia witryny i bywa niezrozumiały dla dzieci nie umiejących czytać;
- każda z aplikacji umożliwia rodzicom wgląd w aktywność dziecka w internecie oraz ustawienie limitów korzystania z globalnej sieci;
- większość filtrów jest wyposażonych w regulację stopnia czułości;
- niemal wszystkie programy dają możliwość utworzenia i modyfikacji niezależnych profili ustawień w zależności od wieku dziecka[77].

Czy wyżej wymienione technologie zapewniają pełną ochronę małoletnim internautom?

Zdaniem członków projektu Youth Protection Roundtable, zapewnienie skutecznej ochrony internautów wymaga: usprawniania technologii wspomagających oraz infrastruktury; zwiększenia użyteczności oprogramowania filtrującego; udoskonalania serwisów internetowych – podstawy technologiczne oraz wprowadzenie dodatkowych *widgetów* pomagających użytkownikom chronić samych siebie oraz uzgodnienia reguł przez usługodawców i operatorów.

Konieczność stosowania w domowych komputerach tzw. programów filtrujących, umożliwiających blokowanie stron zawierających niebezpieczne dla dzieci treści, jest zadaniem rodziców – podkreślił Łukasz Wojtasik – specjalista z NASK. Dodał: „Stosowanie filtrów rodzinnych nie zwalnia jednak dorosłych z odpowiedzialności za bezpieczeństwo dzieci. Nie istnieją bowiem programy, które w 100% zabezpieczałyby dzieci przed dostępem do nieodpowiednich dla nich treści”[78].

Podsumowanie

Problem ochrony dzieci wymaga działania zarówno na arenie krajowej, jak i międzynarodowej. Konieczne jest wdrażanie odpowiednich regulacji prawnych i programów profilaktycznych. Niezbędne jest uświadomienie rodzicom i opiekunom, że internet nie zawsze jest „bezpieczną” formą spędzania czasu wolnego. Potrzebę

[77] *Tamże,* s. 23.

[78] *Internet niebezpieczny dla dzieci,* http://wirtualnemedia.pl/document.php?id=710977 (odczyt z dn. 30 maja 2011 r.).

tę dostrzegli już przedstawiciele instytucji rządowych i pozarządowych. Jednak nie można tej odpowiedzialności przerzucić tylko na badaczy, instytucje rządowe, szkołę czy stowarzyszenia konsumenckie. Nieocenioną i niezastąpioną rolę powinni odegrać rodzice. Ich przykład i postawa są nieocenione.

Literatura

Berson I. R., *Cyberofiary: psychospołeczne konsekwencje wykorzystywania młodzieży za pośrednictwem internetu*, „Dziecko Krzywdzone" 2003, nr 2, s. 72–83.

Boratyński J., *Działania Unii Europejskiej przeciwko wykorzystywaniu seksualnemu dzieci,* Warszawa 2009.

Braun-Gałkowska M., *Oddziaływanie internetu na psychikę dzieci*, „Edukacja Medialna" 2003, nr 3, s. 14–20.

Busch M., *Program unijny Safer Internet – realizowane i planowane działania. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29–30.09.2009 r. Materiały niepublikowane.

Computer Emergency Response Team, www.cert.pl (odczyt z dn. 9 maja 2011 r.).

Croll J., *Rekomendacje wypracowane w ramach projektu Youth Protection Roundtable. Materiały pokonferencyjne,* Warszawa 2009.

Decyzja nr 1351/2008/EC Parlamentu Europejskiego i Rady z dnia 24 grudnia 2008 r. w sprawie kontynuacji wieloletniego programu wspólnotowego na rzecz bezpieczniejszego korzystania z internetu i nowych technologii sieciowych, Dz. Urz. L 348, 24.12.2008.

Decyzja nr 276/1999/WE Parlamentu Europejskiego i Rady z dnia 25 stycznia 1999 r. przyjmująca wieloletni plan działań Wspólnoty w zakresie promowania bezpieczniejszego korzystania z internetu poprzez zwalczanie sprzecznych z prawem i szkodliwych treści w sieciach komputerowych, Dz. Urz. L 33 z 06.02.1999.

Decyzja Ramowa Rady 2004/68/WSiSW z dnia 22 grudnia 2003 r. dotycząca zwalczania seksualnego wykorzystywania dzieci i pornografii dziecięcej, Dz. Urz. L 013 z 20.01.2004.

Dynamiczna Koalicja na rzecz Bezpieczeństwa Dzieci w Internecie, http://www.dzieckowsieci.pl/strona.php?p=116 (odczyt z dn. 9 maja 2011 r.).

Dyrektywa 2010/13/UE Parlamentu Europejskiego i Rady z dnia 10 marca 2010 r. o audiowizualnych usługach medialnych), Dz. Urz. L 95/22 z 15 kwietnia 2010.

Dyżurnet.pl, *Rozwiązania filtrujące niepożądane treści w internecie. Raport Dyżurnet.pl*, Warszawa 2009.

Dyżurnet.pl. *Raport z działalności zespołu w latach 2005–2009*, Warszawa 2010.

Dziecko w sieci – nowe przepisy ułatwią walkę z pedofilią, http://www.wirtualnemedia.pl/artykul/dziecko-w-sieci-nowe-przepisy-ulatwia-walke-z-pedofilia (odczyt z dn. 9 maja 2011 r.).

Fenik K., *Uzależnienie od internetu. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie*; Warszawa 29–30.09.2009 r. Materiały niepublikowane.

Filiciak M., *Nowe wyzwania edukacji medialnej: Web 2.0. Materiały konferencyjne z III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie; Warszawa 29–30.09.2009 r.,* Warszawa 2009.

Fundacja Dzieci Niczyje, www.fdn.pl (odczyt z dn. 27 maja 2011 r.).
Fundacja Kidprotect.pl, www.kidprotect.pl (odczyt z dn. 9 maja 2011 r.).
Guerreschi C, *Nowe uzależnienia*, Kraków 2006.
Helpline.org.pl, http://www.dzieckowsieci.pl/strona.php?p=101 (odczyt z dn. 11 maja 2011 r.).
Historia Dyzurnet.pl, http://www.dyzurnet.pl/o_nas/historia.html (odczyt z dn. 9 maja 2011 r.).
ICRA, www.fosi.org/cms/ (odczyt z dn. 27 maja 2011 r.).
Inicjatywy i raporty Komisji Europejskiej. Sprawozdanie nr 21/2009, http://www.senat.gov.pl/k7/ue/inne/2009/021.pdf (odczyt z dn. 15 maja 2011 r.).
Internet niebezpieczny dla dzieci, http://wirtualnemedia.pl/document.php?id=710977 (odczyt z dn. 30 maja 2011 r.).
Jenkins H., *Kultura konwergencji. Zderzenie starych i nowych mediów*, Warszawa 2007.
J@k w necie? Bezpiecznie!!!. Warsztaty dla klas gimnazjalnych, Warszawa 2009.
Jończyk I., Różycka M., Kurowski K., Węgłowski W., *Jak w necie? Bezpiecznie!,* Warszawa 2007.
Kodeks karny; Ustawa z dnia 6 czerwca 1997 r., Dz.U. z 1997 r. Nr 88, poz. 553 ze zm.
Konstytucja Rzeczypospolitej Polskiej; Ustawa z dnia 2 kwietnia 1997 r., Dz.U. z 1997 r. Nr 78, poz. 483.
Konwencja o Prawach Dziecka z dnia 20 listopada 1989 r., Ustawa w sprawie ratyfikacji Konwencji o Prawach Dziecka z dnia 20 listopada 1989 r., Dz.U. z 1991 r. Nr 120, poz. 526.
Konwencja Rady Europy o Cyberprzestępczości z dnia 23 listopada 2001 r., http://www.ms.gov.pl/ue/ue3in32.shtml (odczyt z dn. 7 maja 2011 r.).
Konwencja Rady Europy o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych z dnia 12 lipca 2007 r., http://www.ms.gov.pl/re/081027_konw.pdf (odczyt z dn. 3 maja 2011 r.).
Kordoń M., *Niebezpieczeństwa sieci*, „Psychologia w Szkole" 2004, nr 2, s. 55–63.
Kosek-Nita S, *Uzależnienie od komputera i jego następstwa*, „Wychowanie na Co Dzień" 2006, nr 3, s. 6–9.
Levina O., *Pomoc ofiarom wykorzystywania seksualnego przez internet w Rosji. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29–30.09.2009r. Materiały niepublikowane.
Lew-Starowicz R., *Nowe rozwiązania legislacyjne w zakresie zwalczania pedofilii i pornografii dziecięcej w internecie. Materiały pokonferencyjne,* Warszawa 2009.
Maj M., *Techniczne aspekty bezpieczeństwa w internecie. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29–30.09.2009r. Materiały niepublikowane.
Naukowa i Akademicka Sieć Komputerowa, www.nask.pl (odczyt z dn. 8 maja 2011 r.).
Palmer T., *Ciemna strona internetu – ofiary pornografii dziecięcej,* „Dziecko Krzywdzone" 2005, nr 13, s. 28–44.
Paradowski K., *Internet: korzyści, zagrożenia: praktyczny poradnik dla nauczycieli, pedagogów, rodziców,* Warszawa 2000.
Projekt Saferinternet.pl, http://www.dzieckowsieci.pl/strona.php?p=75 (odczyt z dn. 10 maja 2011 r.).
Protokół Opcjonalny do Konwencji Narodów Zjednoczonych o Prawach Dziecka dotyczący sprzedaży dzieci, prostytucji dziecięcej i pornografii z udziałem dzieci z dnia 25 maja 2000 r., http://www.vilp.de/p11.htm (odczyt z dn. 8 maja2011 r.).

Pyżalski J., *Agresja elektroniczna dzieci i młodzieży – różne wymiary zjawiska,* „Dziecko Krzywdzone" 2009, nr 29, s. 12- 26.

Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)8 z dnia 31 października 2001 r.: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych, http://www.krrit.gov.pl/bip/Portals/0/publikacje/analizy/Analiza2005_07.pdf (odczyt z dn. 6 maja 2011 r.).

Rozwiązania filtrujące niepożądane treści w internecie. Raport Dyżurnet.pl, Warszawa 2009.

Safer Internet Programme: Empowering and Protecting Children Online, http://ec.europa.eu/information_society/activities/sip/index_en.htm (odczyt z dn. 7 maja 2011 r.).

Safer Internet w Europie, http://www.saferinternet.pl/awereness_w_europie/(odczyt z dn. 2 maja 2011 r.).

Safer Internet, http://ec.europa.eu/information_society/activities/sip/index_en.htm (odczyt z dn. 4 maja 2011 r.).

Saferinternet.pl, www.saferinternet.pl (odczyt z dn. 10 maja 2011 r.).

Serzycki M., *Portale społecznościowe a ochrona danych osobowych. Wykład wygłoszony podczas III Międzynarodowej Konferencji: Bezpieczeństwo dzieci i młodzieży w internecie;* Warszawa 29–30 września 2009r. Materiały niepublikowane.

Stiftung Digitale Chancen, *Zestaw zaleceń projektu Youth Protection Roundtable*, Hamburg 2009.

Śpiewak J., *Aspekty prawne,* http://www.kidprotect.pl/artykuly/?item=1 (odczyt z dn. 3 maja 2011 r.).

Śpiewak J., *Internet a zagrożenia rozwoju dzieci i młodzieży*, w: *Jednostka – grupa – cybersieć. Psychologiczne, społeczno-kulturowe i edukacyjne aspekty społeczeństwa informacyjnego*, red. M. Radochoński, B. Przywara, Rzeszów 2004.

Śpiewak J., *Wykorzystanie seksualne dziecka w kodeksie karnym*, „Niebieska Linia" 2010, nr 3, s. 28–37.

Tęcza-Ćwierz J., *Internet – szanse i zagrożenia,* „Wychowawca" 2003, nr 6, s. 16–17.

Ustawa z dnia 5 listopada 2009 roku o zmianie ustawy – *kodeks karny*, ustawy – *Kodeks postępowania karnego*, ustawy – *Kodeks karny wykonawczy*, ustawy – *Kodeks karny skarbowy*, Dz.U. z 2009 r. Nr 206, poz. 1589.

Ustawa z dnia 19 sierpnia 1994 r. o ochronie zdrowia psychicznego, Dz.U. z 1994 r. Nr 111, poz. 535.

Walrave M., Heirman W., *Skutki cyberbullyingu – oskarżenie czy obrona technologii?,* „Dziecko Krzywdzone" 2009, nr 29, s. 27–36.

Wojtasik Ł., *Pedofilia i pornografia dziecięca w internecie*, „Dziecko Krzywdzone" 2003, nr 2, s. 56–67.

Wojtasik Ł., *Przemoc rówieśnicza z użyciem mediów elektronicznych,* „Dziecko Krzywdzone" 2009, nr 29, s. 7–11.

Wolak J., Mitchell K., Finkelhor G., *Czy nękanie za pośrednictwem internetu jest formą przemocy rówieśniczej? Analiza zjawiska nękania online przez znajomych rówieśników i przez sprawców znanych wyłącznie z sieci,* „Dziecko Krzywdzone" 2009, nr 29, s. 77–89.

Wosińska W., *Terror z komputerów*, „Charaktery" 2005, nr 7, s. 25–26.

Youth Protection Roundtable, http://www.dzieckowsieci.pl/strona.php?p=76 (odczyt z dn. 12 maja2011 r.).

Youth Protection Roundtable, www.yprt.eu (odczyt z dn. 12 maja 2011 r.).

Zalecenie Komisji COM(2009)6464 z dnia 20 sierpnia 2009 r. w sprawie umiejętności korzystania z mediów w środowisku cyfrowym w celu stworzenia bardziej konkurencyjnego sektora audiowizualnego i treści cyfrowych oraz stworzenia integracyjnego społeczeństwa opartego na wiedzy, Dz.U. L 227 z 29 sierpnia 2009.
Zalecenie Parlamentu Europejskiego dla Rady z dnia 3 lutego 2009 r. w sprawie walki z seksualnym wykorzystywaniem dzieci i pornografią dziecięcą, Dz. Urz. L. 12 z 03.02.2009.
Zalecenie Parlamentu Europejskiego i Rady z dnia 20 grudnia 2006 r. w sprawie ochrony małoletnich, godności ludzkiej oraz prawa do odpowiedzi w odniesieniu do konkurencyjności europejskiego przemysłu audiowizualnego oraz internetowych usług informacyjnych, Dz. Urz. L 378 z 27.12.2006.
Zalecenie Rady Europy Rec(2009)5 z dnia 8 lipca 2009 r. w sprawie ochrony dzieci przed szkodliwymi treściami i zachowaniami oraz promowania ich aktywnego uczestnictwa w nowym środowisku informacyjnym i komunikacyjnym, Dz. Urz. L. 29 z 08.07.2009.
Zespół Dyżurnet.pl, www.dyzurnet.pl (odczyt z dn. 27 maja 2011 r.).

The protection of minors in the Internet as a task and challenge for families in the countries of the European Union

Summary

The aim of the publication is to analyze the legal basis for the protection of minors in the Internet, including the regulation of the European Union, the Council of Europe and National Law. In addition, the verification of activities undertaken by the countries of the European Union in the title's scope. An attempt to answer the question of whether the proposed solutions are effective.

After a preliminary theoretical discussion on the risk maps, the main legal regulation for the title's protection (CE Convention on Cybercrime of 23 November 2001, EU Council Framework Decision 2004/68/JHA on combating the sexual exploitation of children and child pornography of 22 December 2003) will be analysed and National Law. The implementation of policy priorities is done through the implementation of aid programs. One of them is Safer Internet. The basic objectives, the main areas for action, assumptions and priorities, implemented initiatives are discussed. The assumptions of the programme of Polish Safer Internet Centre is verified, including the activities of Nobody's Children Foundation and the Research and Academic Computer Network. The tasks and initiatives of the Saferinternet.pl Project (eg the Contact Team: Dyżurnet.pl, so-called hotline and the Aid Team, so-called Helpline.org.pl) will be discussed, the objectives of media and social campaigns (eg Child on the network). The issue of the ability to use the Internet will be analysed. The technical equipment, helping to protect children (project: Youth Protection Roundtable) will be discussed. In this paper the analytical and descriptive method will be used.

Keywords: aid programs, children, education, the European Union, initiatives, internet, law, media protection.