Raport:
Bezpieczeństwo dzieci korzystających z Internetu

na zlecenie Telekomunikacji Polskiej
przygotowała
FUNDACJA DZIECI NICZYJE

we współpracy z ekspertami z:
- Interactive Advertising Bureau Polska
- Agencji Interaktywnej Digital One
- Dyżurnet.pl
- Bebo.com

wrzesień 2008 r.

Spis treści

Wstęp

Internet to nieograniczone źródło wiedzy. W niewiarygodny sposób udoskonalił formy komunikowania się – bez przeszkód możemy rozmawiać, a nawet widzieć się z osobą będącą na drugiej półkuli, a przekaz informacji przebiega w tempie błyskawicznym. Wysłanie maila zajmuje przecież zaledwie kilkanaście sekund. Jednak zawsze należy pamiętać o tym, że w rękach osób nieodpowiedzialnych bądź nieświadomych może okazać się bardzo niebezpiecznym narzędziem do przekazywania bądź rozpowszechniania niebezpiecznych treści, za które uznaje się materiały, mogące mieć szkodliwy wpływ na rozwój i psychikę dziecka (pornografia, rasizm, ksenofobia, treści nawołujące do popełniania przestępstw, zachęcające do prostytucji, do używania narkotyków czy do hazardu oraz takie, które zawierają elementy psychomanipulacji)

Z badania, które na zlecenie Fundacji Dzieci Niczyje przeprowadził Gemius, wynika że 71% dzieci trafia w Internecie na materiały pornograficzne, 51% - na materiały z brutalnymi scenami, a 28% na takie, które propagują przemoc i nietolerancję. Skala problemu jest zatem olbrzymia.
Internet od samego początku to dla środowisk pedofilskich doskonałe narzędzie do dystrybucji, wymiany i produkcji pornografii dziecięcej. Co więcej – pedofile często podając się za rówieśników, dopuszczają się uwodzenia *on-line* małoletnich użytkowników Sieci. To zjawisko, z angielska nazwane *grooming*, dotyczy zwierania znajomości za pomocą mediów elektronicznych, typu: komunikatory, blogi, czaty etc. 64% badanych dzieci przyznaje się do zawierania znajomości w Internecie, z czego 68% otrzymało od nowo poznanej osoby propozycję spotkania w rzeczywistym świecie, a 44,6% - skorzystało z takiego zaproszenia! Naturalnie nie każda znajomość zawarta przy udziale Internetu i nie każde spotkanie, będące skutkiem takiego zdarzenia, nosi znamiona przestępstwa. Niestety jednak większość incydentów z kategorii wykorzystywania dzieci za pośrednictwem Internetu nie zostaje ujawniona, głównie ze względu na drażliwość tematu.

Obok problemu pornografii czy uwodzenia istnieje jeszcze kwestia cyberbullingu, czyli cyberprzemocy rówieśniczej przy użyciu nowych technologii. Często nie zdając sobie sprawy z konsekwencji, dzieci rozsyłają materiały ośmieszające bądź poniżające swoich kolegów. Różnego rodzaju czaty, fora, jak również komunikatory czy SMS'y lub MMS'y stają się narzędziem do dystrybucji kompromitujących treści, np. zdjęć czy filmów. Co drugie badane dziecko twierdzi, że doznało w Internecie wulgarnego wyzywania, a 14% zgłasza przypadki rozpowszechniania przez osoby trzecie kompromitujących materiałów na swój temat. Należy pamiętać, że dzieci narażone są na tego rodzaju niebezpieczeństwa szczególnie, gdyż bardzo chętnie same udostępniają swoje dane

osobowe oraz zdjęcia. Bez problemu zdradzają adres nie tylko e-mail ale i domowy, a także dzielą się zdjęciami z nieznajomymi. W konsekwencji czego padają ofiarami zarówno ceberbullingu jak i różnego rodzaju oszustw, wyłudzeń, kradzieży etc.

Najważniejszym elementem chroniącym dziecko przed szkodliwymi treściami w Internecie powinni być rodzice. Niestety przeważająca większość nie ma pojęcia, z jakiego rodzaju treściami w Internecie ma kontakt jego dziecko. Wprawdzie ponad 70% rodziców uznaje Internet za niebezpieczny, jednak blisko 30% z nich nie potrafi zdefiniować zagrożeń, ani wskazać miejsc, w których można trafić na nieodpowiednie treści. Prawie 60% badanych rodziców nie widzi zagrożeń w korzystaniu z komunikatorów, blisko 40% - w zakupach on-line. Jeśli chodzi o nawiązywanie znajomości przez Internet, czy zamieszczanie zdjęć, rodzice wydają się być bardziej ostrożni, ok. 82% rodziców widzi w tych czynnościach potencjalne niebezpieczeństwo. Jednakowoż 27% dzieci przyznaje, że rodziców nigdy nie interesowało to, czym zajmują się w Internecie. Stalą kontrolę rodzicielską deklaruje zaledwie 10% respondentów. Dlatego ogromną część działań profilaktycznych powinno się prowadzić na poziomie edukacji. Uświadamianie niebezpieczeństwa, wskazywanie miejsc, w których dzieci są najbardziej narażone, a także prezentowanie sposobów przeciwdziałania to podstawowe zagadnienia profilaktycznych programów edukacyjnych zarówno dla dzieci jak i dorosłych – rodziców, nauczycieli czy wychowawców.

Ze względu na różnorodność form zjawiska cyberprzemocy nie zawsze kwestie te regulowane są w kodeksie karnym. W niektórych przypadkach jedynym sposobem ochrony prawnej jest droga cywilna czyli droga roszczeń odszkodowawczych. Brakuje odpowiednich przepisów, na przykład takich, które zapewnią możliwość stosowania przez policję narzędzia prowokacji w zakresie spraw dotyczących przestępstw seksualnych wobec dzieci, w tym szczególnie przestępstw z wykorzystaniem Internetu.

W kwestii bezpieczeństwa dzieci w Sieci wiele zależy również od producentów sprzętu elektronicznego i oprogramowania, a także od samych dostawców usług internetowych. Filtrowanie treści na poziomie sieci dostępowej realizowane przez dostawców, to według ekspertów, jeden z najskuteczniejszych sposobów ochrony. Warto jednak pamiętać, że poza nakładami finansowymi taka realizacja wymaga również odpowiednich uregulowań prawnych.

Niniejszy Raport przedstawia szczegółowe dane pochodzące z badań przeprowadzonych przez Gemiusa na zlecenie Fundacji Dzieci Niczyje, obrazujące skalę a także dokładny obraz problemu. Raport zawiera również komentarze ekspertów oraz wskazuje postulowane kierunki zmian.

I. Jak dzieci korzystają z Internetu

Dzieci i młodzież stanowią zdecydowana większość użytkowników Internetu w Polsce. Większość z nich zaczyna korzystać z Sieci będąc w wieku od 5 do 9 lat (58%) a co szóste z nich swoja przygodę z internetem rozpoczyna już od 4 roku życia lub jeszcze wcześniej (16,1%) [1]!

Żeby skutecznie zadbać o bezpieczeństwo młodych internautów niezbędna jest wiedza na temat tego w jaki sposób korzystają oni z Sieci oraz jaka jest ich opinia i doświadczenia związane z zagrożeniami *online*. Informacji takich dostarczają nieliczne badania realizowane w ostatnich latach wśród dzieci w Polsce. Wśród nich na największą uwagę zasługuje badanie Megapanel PBI/Gemius[2] zrealizowane w listopadzie 2007 roku na grupie ponad 17 tysięcy internautów, na podstawie którego opracowany został raport "Dzieci aktywne *on-line*" analizujący aktywności *on-line* użytkowników Sieci w wieku od 7-14 lat.[3] Z badań i raportu wynikają następujące ustalenia:

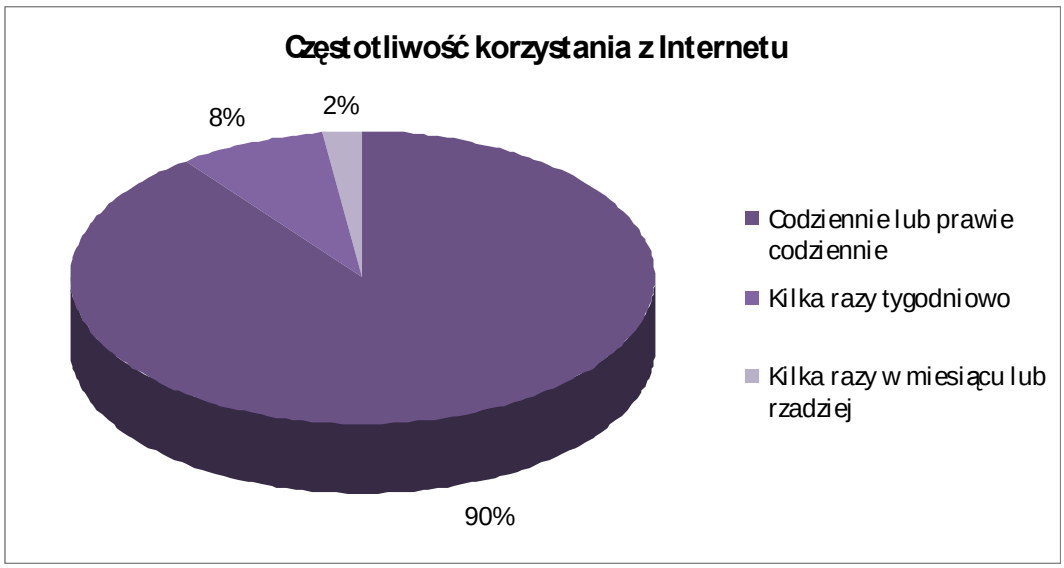
- Dzieci w wieku 7-14 lat stanowią 11% ogółu użytkowników Internetu w Polsce. Szacowana liczba użytkowników Internetu w tym wieku to 1,5 miliona. Najliczniejszą grupę Internautów stanowi młodzież w wieku 15-24 lata (37,7%, ponad 4,630 tys.).

- Dzieci spędzają w Sieci coraz więcej czasu. W ciągu roku (od IV 2006 do IV 2007) czas średni czas poświęcany przez nie w miesiącu na serfowanie wzrósł z 15 godzin, 56 minut do 24 godzin, 27 minut. Najwięcej czasu spędzają w Sieci dzieci w dużych aglomeracji miejskich (33 godziny 42 minuty)

- Niemal co drugie dziecko (45%) korzysta z Internetu codziennie lub prawie codziennie. Co trzecie dziecko (34%) korzysta z Internetu kilka razy w tygodniu.

[1] Badanie „Dzieci online w oczach rodziców", Gemius S.A. dla FDN, luty 2008 r., Próba: rodzice dzieci w wieku 5-15 lat, N=1235

[2] Badanie Gemius SA, Megapanel PBI/Gemius, listopad 2007 r. Liczebność próby: N=17 512. Próba: 7+. Do badania wykorzystano dane o strukturze demograficznej pochodzące z badania NetTrack Millward Brown SMG/KRC.



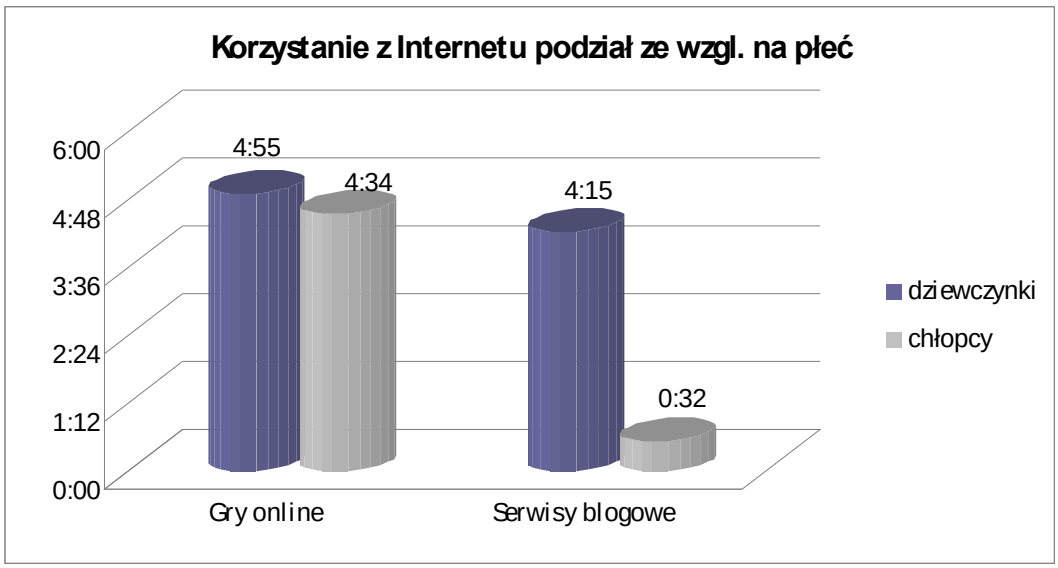
Na podst. badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badania dzieci 12-17lat- N=1779

- Dziewczynki spędzają w Internecie dużo więcej czasu niż chłopcy. Średnio miesięcznie dziewczynki w wieku7-14 lat (47% populacji) serfują 29 godzin, 40 minut a chłopcy (53% populacji) 19 godzin 46 minut.

- Największa popularnością wśród dzieci cieszą się witryny z kategorii „Kultura i rozrywka" - 6 godzin 55 minut miesięcznie. Kolejne kategorie tematyczne odwiedzanych przez dzieci najczęściej witryn to „Nowe technologie" i „Społeczności"

- 70% internautów w wieku 7-14 lat korzysta z możliwości grania *on-line*. Ta grupa wiekowa gra *on-line* najczęściej. Druga w kolejności jest młodzież w wieku 15-24 lata (55%). Wbrew stereotypom dziewczynki poświęcają na gry *on-line* nieco więcej czasu (4 godziny, 55 minut)

niż chłopcy (4 godziny, 34 minuty)



Na podst. badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badania dzieci 12-17lat- N=1779

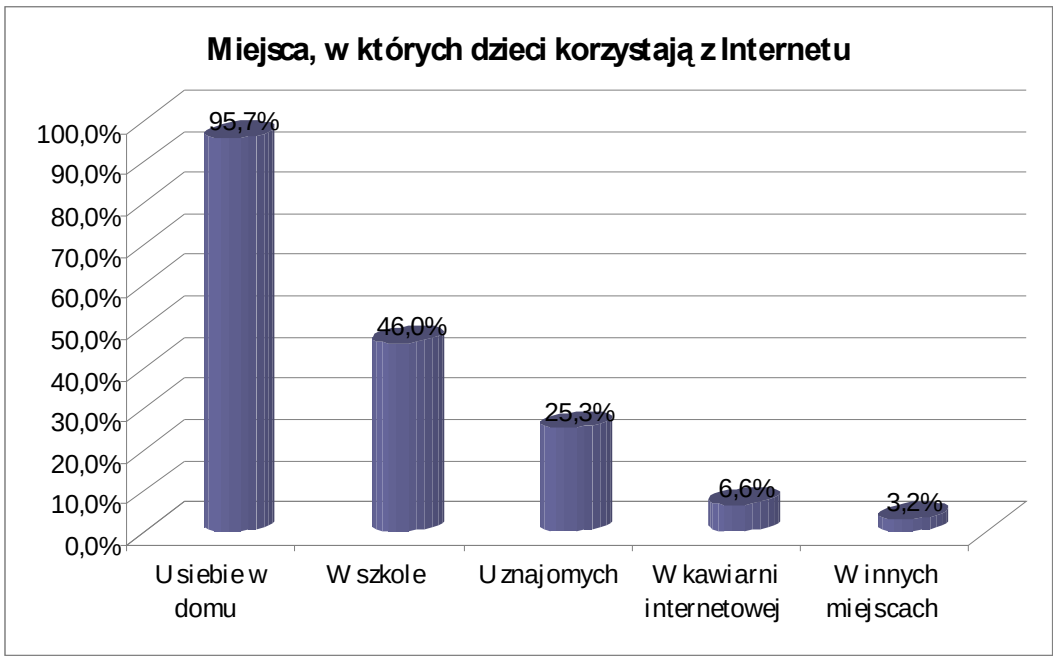
- 40 % dzieci ma kontakt z pornografią. Miesięcznie dzieci spędzają na eksplorowaniu serwisów erotycznych średnio ok. godziny (57 min 36 s – średni czas w czerwcu 2007 r.)

- Niemal co drugie dziecko aktywne *on-line* odwiedza serwisy blogowe. Przy czym dziewczynki spędzają „na blogach" zdecydowanie więcej czasu (4 godziny 15 minut) niż chłopcy (32 minuty)

Z pozostałych danych badawczych warte odnotowania są następujące dane[4]:

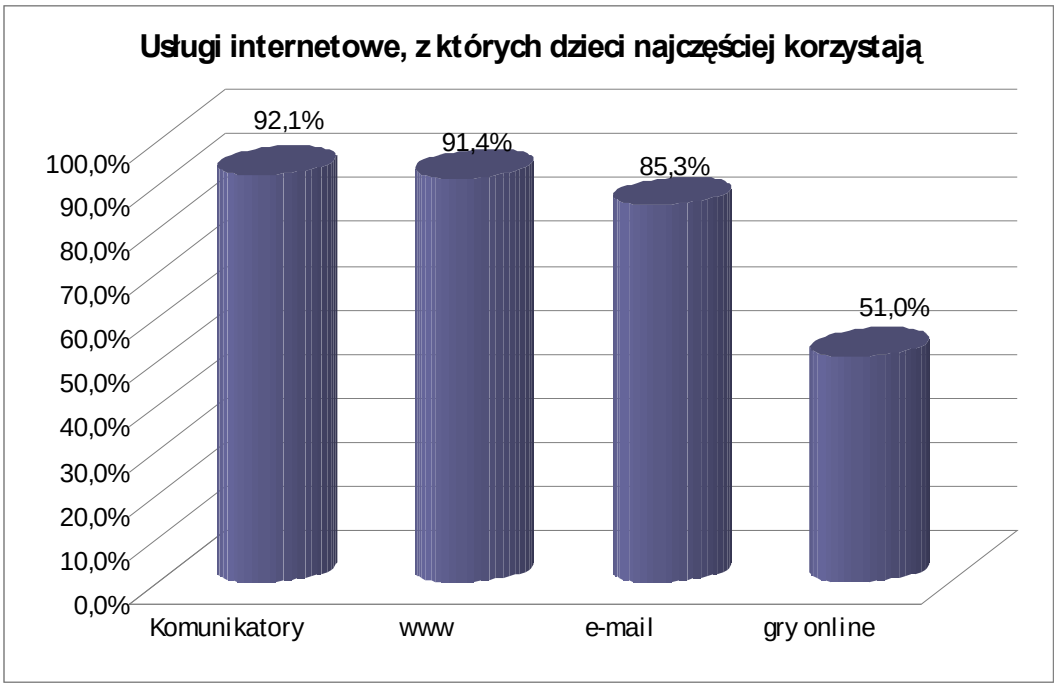
- Zdecydowana większość dzieci w wieku 12-17 lat korzysta z Internetu u siebie w domu (95,7%) . Drugim miejscem, pod względem liczby wskazań, jest szkoła – 46,0%. Co czwarte dziecko korzysta z Internetu u znajomych (25,3%).

[4] Poniższe dane pochodzą z badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badani: dzieci 12-17 lat - N=1779



Na podst. badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badania dzieci 12-17lat- N=1779

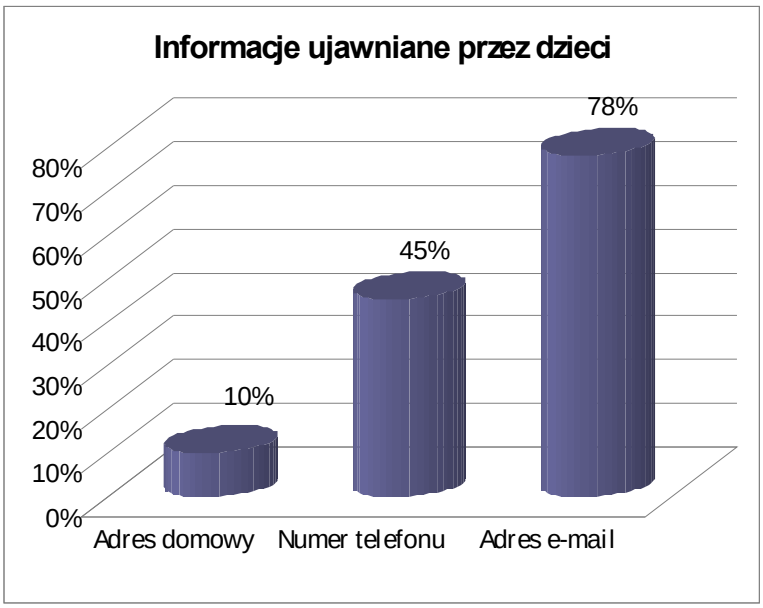
- Dzieci (12-17 lat) najczęściej korzystają z takich usług internetowych jak: komunikatory - 92,1%, strony WWW – 91,4%, poczta e-mail – 85,3%, gry *on-line* 51%. Najbardziej dynamiczny jest przyrost użytkowników gier *on-line*.



Na podst. badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badania dzieci 12-17lat- N=1779

- 38% dzieci korzystających z komunikatorów wykorzystuje funkcję komunikacji głosowej.

- 64% dzieci zawiera znajomości w Internecie znajomości! Znaczna część spośród nich przekazuje osobom poznanym w Internecie prywatne informacje o sobie, jak adres domowy (10%), numer telefonu (45%) adres e-mail (78%). Ponad 58% dzieci wysłało osobie poznanej w Sieci swoje zdjęcie (47, 4% robi to regularnie)



Na podst. badania „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badania dzieci 12-17lat- N=1779

II. Zagrożenia związane z korzystaniem przez dzieci z Internetu – charakterystyka i skala zjawiska.

„Dlaczego bezpieczeństwo dzieci w Internecie jest takie ważne? Ponieważ Internet, jak każda ludzka aktywność, ma swoje dobre i złe strony. Nie ma co ukrywać, to trochę jak w życiu. Jeśli pójdziemy w ciemny zaułek, ryzykujemy, że dostaniemy po głowie. W Internecie jest podobnie. Skoro sieć działa na wszystkich polach ludzkiej aktywności, oznacza to, że funkcjonuje i na tych, z którymi na co dzień walczymy. Dlatego tak ważne jest, by z Internetu korzystać... mądrze.

Jako osoba od ponad dekady pracująca w branży internetowej, dostrzegam wiele pozytywnych aspektów Internetu. Z przyjemnością obserwowałem, jak zmieniała się konsumpcja tego medium, jak Internet wpływał na kształtowanie postaw ludzi i jak silnie oddziaływał na nasz sposób nauki, pracy, komunikacji, spędzania wolnego czasu czy wreszcie prowadzenia biznesu. Jednocześnie zawsze byłem w pełni świadomy zagrożeń, jakie Internet ze sobą niesie – zarówno ze strony ludzi, którzy z niego korzystają, jak i publikowanych tam treści i dostępnych narzędzi.

Tym bardziej, od momentu rozpoczęcia swojej działalności w ramach Związku Pracodawców Branży Internetowej IAB Polska, jestem zwolennikiem brania przez branżę odpowiedzialności za sprawy związane z bezpieczeństwem użytkowników sieci, a w szczególności tych najmłodszych. IAB stara się aktywnie wspomagać inicjatywy pozwalające poprawić bezpieczeństwo korzystania z Internetu, propagujące tego typu działania i kładące nacisk na edukację oraz kształtowanie odpowiednich postaw rodziców i dzieci w Internecie.

Niestety, przeniesienie na branżę odpowiedzialności za bezpieczeństwo dzieci w Internecie nie jest wystarczające. To ogromnie istotne, aby świadomość zagrożeń była również po stronie rodziców. Wszyscy zdajemy sobie bowiem sprawę z tego, że przestępcy istnieją w świecie rzeczywistym. Niestety, jeżeli o chodzi o przestępczość wirtualną, to jej świadomość nie jest już tak wysoka, zwłaszcza wśród rodziców małych dzieci i młodzieży. Rodzic przestrzega swoje dziecko np. przed wsiadaniem do samochodu z obcą osobą, nie zawsze jednak potrafi przestrzec przed tym, żeby dziecko nie podawało swoich danych osobowych w Internecie. Wielu rodziców nie kontroluje także tego, z jakich stron WWW korzystają ich dzieci, jakich treści poszukują, z kim rozmawiają. Dlatego w przypadku zwalczania przestępstw internetowych niezwykle ważna jest edukacja.

I na koniec – bardziej osobiście. Jako ojciec przyszłej młodej użytkowniczki Internetu, mam do kwestii bezpieczeństwa w sieci bardzo emocjonalne podejście. Moja córka prędzej czy później będzie miała styczność z Internetem. Chciałbym więc, aby była świadoma możliwości, jakie daje to medium oraz zagrożeń, jakie za sobą niesie. Wiem jednak, że nie można całej odpowiedzialności zrzucać na „zły" Internet. To medium to dla mnie wciąż niezwykle przydatne i wielofunkcyjne narzędzie – przez Internet można rozmawiać ze znajomymi z całego świata, poznawać nowych ludzi i nowe kultury, można tworzyć współpracujące ze sobą grupy, docierać do

treści, utworów, multimediów niedostępnych w sklepach czy lokalnych bibliotekach, w końcu – wyrażać siebie. Wierzę więc, że w kwestii bezpieczeństwa w sieci wiele można zrobić, jeśli położymy nacisk na edukację i pokazywanie oraz utrwalanie pozytywnych wzorców już od najmłodszych lat. W związku z tym będę się starał nauczyć moją córkę, jak bezpiecznie korzystać z olbrzymich możliwości Internetu – tak samo jak będę uczył ją, by nie wsiadała do samochodu z nieznajomą osobą.".

Michał Tober

Prezes IAB Polska

Intensywny rozwój Internetu i coraz większa dostępność do sieci dzieci i młodzieży, poza wszelkimi pozytywami , wiąże się z coraz większym repertuarem i rosnącą skalą zagrożeń. Za najpoważniejsze z nich uznaje się najczęściej zjawiska związane z szeroko rozumianym wykorzystywaniem seksualnym dzieci. Od samego początku Internet wykorzystywany jest przez środowiska pedofilskie w celach dystrybucji, wymiany i produkcji pornografii dziecięcej. Rok rocznie ofiarami tego procederu pada na całym świecie tysiące dzieci, a do Sieci trafiają niezliczone ilości materiałów pornograficznych z ich udziałem. Wraz z rozwojem serwisów komunikacyjnych problemem stało się również uwodzenie dzieci w Internecie, prowadzące często do wykorzystania seksualnego w rzeczywistym świecie. Dzieci coraz częściej wikłane są również w proceder prostytucji w Sieci.

Poza zjawiskiem pedofilii dzieci narażone są w Internecie na szereg innych zagrożeń. Ze względu na szerokie spektrum tych zjawisk, na potrzeby niniejszego raportu proponowana jest następująca typologia, uwzględniająca specyficzne i najpoważniejsze zagrożenia dla najmłodszych internautów:

- **Niebezpieczne kontakty w Sieci**
- **Kontakty z niebezpiecznymi treściami**
- **Cyberprzemoc (przemoc rówieśnicza)**

2.1 Niebezpieczne kontakty w Sieci

Młodzi internauci często korzystają w Sieci z serwisów komunikacyjnych oraz serwisów społecznościowych i zawierają w Internecie znajomości. Kontakty *on-line* mogą stanowić dla dzieci poważne zagrożenie, szczególnie w sytuacji kiedy prowadzą do spotkania w rzeczywistym świecie. Możliwości Sieci wykorzystują między innymi pedofile. Zjawisko uwodzenia dzieci *on-line*, określane w anglojęzycznej literaturze przedmiotu terminem *grooming*, dostrzeżone zostało już w latach dziewięćdziesiątych a skala problemu rośnie wraz z rozwojem serwisów komunikacyjnych i przyrostem populacji dzieci korzystających z Internetu. W procesie *grooming'*u pedofile poddają dzieci psychomanipulacji,. Czasami elementem uwodzenia jest udawanie rówieśnika potencjalnej ofiary, przynajmniej w pierwszym etapie relacji. Jednak, wbrew stereotypowememu wyobrażeniu, przypadki takie należą do rzadkości a sprawcy wykorzystywania seksualnego dzieci najczęściej nie ukrywają w kontaktach *on-line* przed dzieckiem ani swojego wieku ani intencji, sprawnie manipulując ofiarą.

Zdarza się, że kontakty seksualne pomiędzy nieletnim a dorosłym inicjowane są przez dziecko. Anonse młodych internautów, wskazujące na gotowość do takiej relacji, znaleźć można w serwisach randkowych czy czatowych (czasami z informacją o oczekiwanej gratyfikacji). Należy podkreślić, że okoliczność taka w żadnym stopniu nie zwalnia sprawcy z moralnej i karnej odpowiedzialności za popełnione przestępstwo.

Młodzi internauci narażeni są w Sieci również na kontakty z innymi niebezpiecznymi osobami, jak przedstawiciele rozmaitych sekt, ruchów neonazistowskich itp. Niebezpiecznym zjawiskiem coraz częściej odnotowywanym w Sieci jest nakłanianie młodych ludzi do popełniania samobójstw!

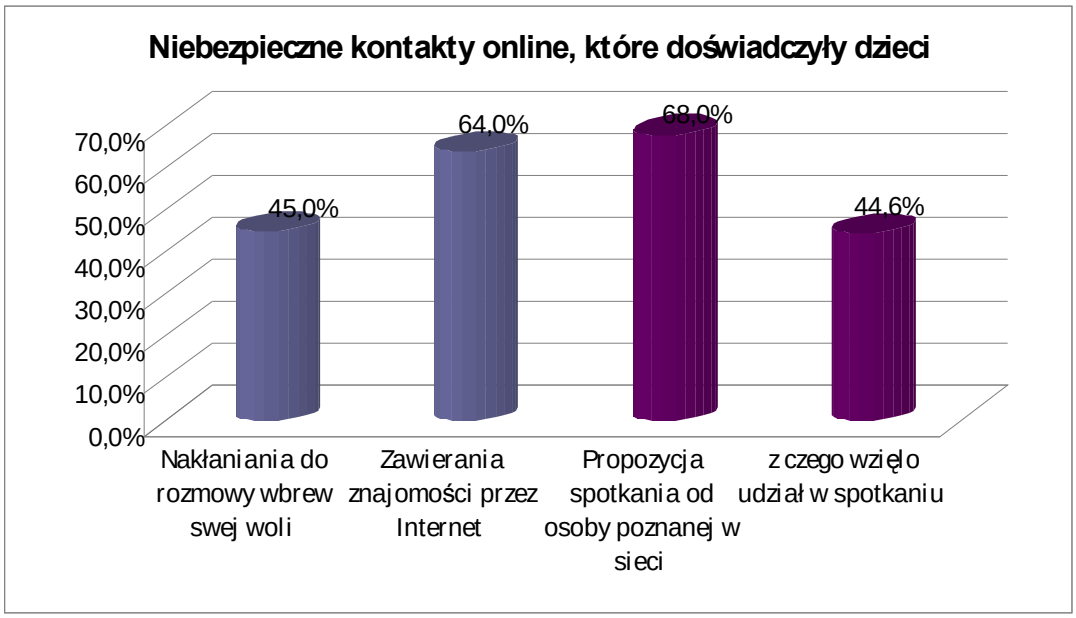
Skala problemu:

Skala niebezpiecznych kontaktów *on-line* i związanych z nimi przestępstw popełnianych w rzeczywistym świecie trudna jest do oszacowania. Statystyki policyjne nie są pomocne, gdyż nie odnotowują, że do przestępstwa, np. wykorzystywania seksualnego dziecka, doszło przy użyciu Internetu. Poza tym zdecydowana większość takich przypadków pozostaje nieujawniona, szczególnie jeżeli dochodzi do nich za przyzwoleniem ofiary. Wycinek problemu pokazują media, ale dotyczy to jedynie ujawnionych i spektakularnych przypadków. Ze względu na drażliwość tematu i jego ograniczoną skalę informacje takie trudno też uzyskać w toku badań socjologicznych.

Informacje o potencjale zagrożeń związanych z kontakami *on-line* z obcymi osobami w Sieci pokazują wyniki badań „Dziecko w Sieci" przeprowadzonych w 2006 roku przez Fundację Dzieci Niczyje i firmę badawczą Gemius S.A.

Najważniejsze ustalenia badawcze[5]:

- 45% młodych internautów nakłanianych było w Sieci, wbrew swojej woli, przez obce osoby do rozmowy. Co piąte dziecko taka sytuacja przestraszyła.
- 64% dzieci korzystających z Sieci zawiera w niej znajomości
- 68% spośród nich co najmniej raz otrzymało od osoby poznanej w Sieci propozycję spotkania; 44,6% dzieci wzięło udział w spotkaniu!



„Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badani: dzieci 12-17 lat - N=1779

- Dzieci zawierające w Sieci znajomości podają obcym dane osobowe, jak adres domowy (10%), numer telefonu (45%) adres e-mail (78%). Ponad 58% z nich wysłało osobie poznanej w Sieci swoje zdjęcie
- Jedynie 23,6% dzieci informuje rodziców o spotkaniach z osobami poznanymi w Sieci.
- Połowa dzieci uczestniczy w spotkaniach w pojedynkę.

[5] „Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badani: dzieci 12-17 lat - N=1779

2.2 Kontakty z niebezpiecznymi treściami

Mianem niebezpiecznych treści w Internecie (ang. *harmful content*) określa się materiały, które mogą mieć szkodliwy wpływ na rozwój i psychikę dziecka. Część materiałów o takim charakterze, jak pornografia dziecięca, rasizm, ksenofobia jest niezgodna z prawem, inne prezentowane są w Sieci legalnie.

Jedna z przyjętych typologii problemu wyróżnia:[6]

- Treści prezentujące przemoc, pornografię;
- Treści propagujące rasizm i ksenofobię;
- Treści nawołujące do popełnienia przestępstwa;
- Treści promujące faszystowski lub inny totalitarny ustrój państwa;
- Treści zachęcające do prostytucji, używania narkotyków czy hazardu;
- Treści zawierające elementy psychomanipulacji (np. namawiające do przystąpienia do sekty);

Najliczniej reprezentowaną w Sieci kategorią niebezpiecznych treści jest pornografia. Co prawda serwisy pornograficzne formalnie działają w sieci legalnie, jednak częsty brak odpowiednich informacji przestrzegających przed ich zawartością, a tym bardziej promocja tych serwisów w Sieci, trafiająca również do dzieci, powoduje częsty kontakt młodych internautów z takimi materiałami a właścicieli serwisów naraża na zarzut narzucania nieletnim treści pornograficznych, co zgodnie z obowiązującym w Polsce prawem jest przestępstwem.

Skala problemu:

W 2007 roku na potrzeby kampanii społecznej „Dziecko w Sieci" agencja Gemius S.A. przeprowadziła badania, dotyczące kontaktów dzieci z niebezpiecznymi treściami[7]:

- 71% dzieci trafia na materiały pornograficzne (63% przypadkowo)
- 51% dzieci trafiła na materiały z brutalnymi scenami przemocy (61% przypadkowo)
- 28% dzieci trafiło na materiały propagujące przemoc i nietolerancje (74% przypadkowo)

[6] Źródło: www.dzieckowsieci.pl

[7] „Kontakty dzieci z niebezpiecznymi treściami w Internecie" Gemius S.A., FDN, wrzesień 2006, badani: dzieci 12-17 lat, N=2559

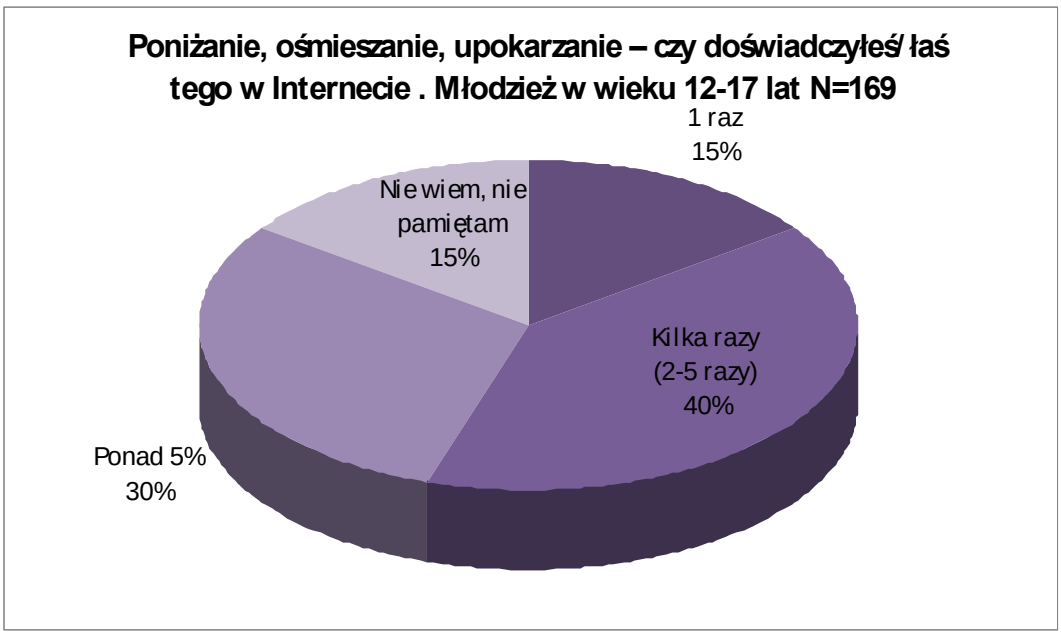
- Co czwarte dziecko deklaruje, że rodzice nigdy nie interesują się tym, co robi w Internecie
- Jedynie 10% dzieci deklaruje regularną opiekę rodziców podczas korzystania z Sieci.

Inne badania pokazują niepokojąco wysoki odsetek kontaktów z pornografią najmłodszych użytkowników Internetu. Z materiałami o takim charakterze spotkało się 40% dzieci w wieku od 7 do 14 lat.[8]

2.3 Cyberprzemoc (przemoc rówieśnicza)

Zjawisko cyberprzemocy najkrócej definiuje się jako przemoc z użyciem technologii informacyjnych i komunikacyjnych. Owe technologie to głównie Internet oraz telefony komórkowe. Część definicji ogranicza stosowanie terminu „cyberbullying", czy „cyberprzemoc" wyłącznie do przemocy rówieśniczej, inne nie stawiają ograniczeń wiekowych, nie wątpliwie jednak najczęściej terminów tych używa się właśnie w kontekście przemocy wśród najmłodszych. Podstawowe formy zjawiska to:

- nękanie, straszenie, szantażowanie z użyciem Sieci,
- publikowanie lub rozsyłanie ośmieszających, kompromitujących informacji, zdjęć, filmów z użyciem Sieci
- podszywanie się w Sieci pod kogoś wbrew jego woli.



[8] Raport "Dzieci aktywne online" , Gemius 2007

Źródło: gemiusAdHoc, styczeń 2007

Do działań określanych mianem cyberprzemocy wykorzystywane są głównie: poczta elektroniczna, czaty, komunikatory, strony internetowe, blogi, serwisy społecznościowe, grupy dyskusyjne, serwisy SMS i MMS.

W odróżnieniu od „tradycyjnej" przemocy (ang *bullying*) zjawisko cyberprzemocy charakteryzuje wysoki poziom anonimowości sprawcy. Ponadto na znaczeniu traci klasycznie rozumiana „siła", mierzona cechami fizycznymi, czy społecznymi a atutem sprawcy staje się umiejętność wykorzystywania możliwości, jakie dają media elektroniczne. Charakterystyczna dla problemu szybkość rozpowszechniania materiałów kierowanych przeciwko ofierze oraz ich powszechna dostępność w Sieci sprawiają, że jest zjawisko szczególnie niebezpieczne. Kompromitujące zdjęcia, filmy czy informacje potrafią zrobić w Internecie bardzo szybką „karierę" a ich usunięcie jest często praktycznie nie możliwe. Dodatkową uciążliwością dla ofiar cyberprzemocy jest stałe narażenie na atak, niezależnie od miejsca czy pory dnia lub nocy. Kolejną ważną cechą problemu jest stosunkowo niski poziom kontroli społecznej tego typu zachowań. Sytuacja doznawania przez dziecko krzywdy za pośrednictwem mediów elektronicznych jest często trudna do zaobserwowania przez rodziców, czy nauczycieli, szczególnie jeżeli maja oni ograniczoną wiedzę i doświadczenia związane z korzystaniem z mediów elektronicznych.

Skala problemu:

Problem cyberprzemocy rozpoznany został w Polsce na początku 2007 roku przez Fundację Dzieci Niczyje i firmę badawczą Gemius S.A.. W toku badań *„Przemoc rówieśnicza a media elektroniczne"* dzieci pytane były o doświadczenia następujących sytuacji:

- Przemoc werbalna w sieci (wulgarne wyzywanie, poniżanie, ośmieszanie, straszenie, szantaż)
- Rejestrowanie filmów i zdjęć wbrew woli dziecka
- Publikowanie w sieci filmów, zdjęć i informacji ośmieszających dziecko
- Podszywanie się w sieci pod dziecko

Respondenci pytani byli również o ich odczucia i reakcję w danej sytuacji oraz proszeni o próbę określenia sprawcy zdarzenia.

Najważniejsze ustalenia badawcze[9]:

- Co drugi młody człowiek (52%) miał do czynienia z przemocą werbalną w Internecie lub poprzez telefon komórkowy. 47% dzieci doświadczyło wulgarnego wyzywania; 21%, poniżania, ośmieszania i upokarzania; 16% straszenia i szantażowana.
- 29% dzieci zgłasza, że ktoś w Sieci podawał się za nie wbrew ich woli.
- Ponad połowa (57%) osób w wieku 12-17 była przynajmniej raz obiektem zdjęć lub filmów wykonanych wbrew ich woli.
- 14% dzieci zgłasza przypadki rozpowszechniania za pośrednictwem Internetu lub GSM kompromitujących je materiałów.
- Akty cyberprzemocy często powodują u ofiar irytację, lęk i zawstydzenie.

2.4 Inne zagrożenia

Poza zagrożeniami specyficznymi dla młodych internautów, dzieci narażone są w Sieci na szereg innych niebezpieczeństw, właściwych również dla dorosłych użytkowników Internetu. Wśród nich na uwagę zasługują sytuacje określane mianem **cyberprzestępczości** (ang. *cyber-crime, computer crime*), czyli przestępstw związanych z komputerem i Internetem i ukierunkowanych na systemy i dane komputerowe, takich jak włamania do systemów komputerowych (hacking, cracking), nielegalne kopiowanie i rozpowszechnianie programów komputerowych (piractwo), nieuprawnione niszczenie danych komputerowych itp. Należy mieć na uwadze, że dzieci jako użytkownicy Internetu i komputera padają ofiarami takich przestępstw, ale również często są ich sprawcami.

Dzieci korzystające z Sieci narażone są też na konsekwencje **tradycyjnych przestępstw,** takich jak kradzieże, oszustwa czy wyłudzenia. Internet niezmiernie sprzyja tego typu przestępczości, a dzieci z racji na rosnącą aktywność konsumencką *on-lin*e stają się coraz częściej ofiarami takich przestępstw. Należy jednak pamiętać o występowaniu dzieci w charakterze sprawców oraz konsekwencjach z tym związanymi.

Internet, to również **problem uzależnień**. Z dostępnych badań wynika, że dzieci spędzają w Sieci coraz więcej czasu. Przy tym często pozbawione są kontroli rodzicielskiej. Coraz większą popularnością wśród najmłodszych cieszą się gry *on-line*, szczególnie sprzyjające uzależnieniu od

[9] „Przemoc rówieśnicza a media elektroniczne", Gemius S.A., FDN, luty 2007, badani: dzieci 12-17 lat, N=891).

Internetu. Sytuacja taka, często bagatelizowana przez dorosłych, powodować może poważne konsekwencje takie, jak dezadaptacja społeczna, problemy w nauce, czy problemy zdrowotne.

2.5 Wiedza, opinie i doświadczenia rodziców

Rodziców uznać należy za najważniejsze ogniwo w systemie bezpieczeństwa dzieci w Internecie. Od wiedzy opiekunów dziecka w problematyce zagrożeń internetowych, od tego czy ustalą oni z dzieckiem zasady korzystania z Sieci i czy będą reagować na potencjalnie niebezpieczne sytuacje zależy bezpieczeństwo młodego internauty. Informacje o postawach i wiedzy rodziców w zakresie bezpieczeństwa dzieci w Sieci powinny być również podstawą do projektowania odpowiednich programów profilaktycznych. Problematyka ta rzadko pojawia się w badaniach socjologicznych[10], tym niemniej są dostępne na ten temat interesujące informacje badawcze:[11]

- Zdecydowana większość rodziców uznaje Internet za potencjalnie niebezpieczny da najmłodszych (71,6%). Jednak blisko co trzeci rodzic nie potrafi wskazać na jakiekolwiek zagrożenia dzieci w Internecie (28,4%).

- Stosunkowo duża grupa rodziców nie dostrzega zagrożeń w zachowaniach dzieci, które uznać należy za potencjalnie niebezpieczne, jak: korzystanie z komunikatorów (58,2%), zakupy *on-line* (39,8%), zamieszczanie swoich zdjęć w Internecie (18,2%), poznawanie nowych osób przez Internet (17,5%).

- Wyobrażenia rodziców na temat doświadczeń dzieci w Internecie nie zawsze zbliżone są do stanu faktycznego. Jedynie 11% rodziców dzieci korzystających z Internetu twierdzi, że ich dziecko korzystało z serwisów erotycznych, podczas gdy inne badania potwierdzają, że z serwisów takich zdarza się korzystać 40% młodych internautów. Podobnie jest w przypadku podawania w Sieci danych osobowych takich, jak numer

[10] Problematyka będzie przedmiotem badań „Rodzice wobec zagrożeń dzieci w Internecie" opracowanych przez FDN we współpracy z Fundacją Grupy TP. Badania zrealizowane zostaną metodą ankiety telefonicznej wśród 500 rodziców dzieci w wieku 7-15 lat przez TNS OBOP we wrześniu 2008 roku. Raport z badań opublikowany zostanie m.in. w serwisie www.dzieckowsieci.pl.

[11] Prezentowane niżej dane pochodzą z następujących badań:
„Dzieci online w oczach rodziców", Gemius S.A. dla FDN, luty 2008 r., badani : rodzice dzieci w wieku 5-15 lat, N=1235
„Kontakty dzieci z niebezpiecznymi treściami w Internecie" Gemius S.A., FDN, wrzesień 2006, badani: dzieci 12-17 lat, N=2559
„Dziecko w Sieci" Gemius S.A., FDN, styczeń 2006, badani: dzieci 12-17 lat - N=1779
Gemius SA, Megapanel PBI/Gemius, listopad 2007 r. Liczebność próby: N=17 512.badani: 7+.

telefonu (9% - wyobrażenia rodziców vs. 45% - deklaracje dzieci), czy adresu email (17% vs. 7,9%).

- Co czwarte dziecko zgłasza, że rodzice nigdy nie interesują się tym co robi w Internecie (27%)! Jedynie 10% respondentów deklaruje stałą opiekę rodziców podczas korzystania z Sieci.

- Rodzice stosunkowo rzadko podejmują aktywności na rzecz ograniczenia zagrożeń związanych z korzystaniem z Internetu przez dzieci. Mniej niż połowa z nich kontroluje czas spędzany przez dziecko w Sieci (48,6%), jeszcze mniej (41,9%) kontroluje, co dziecko robi w Sieci. Oprogramowanie filtrujące wykorzystywane jest w co trzeciej rodzinie (33.6%). Zaledwie 16% rodziców towarzyszy dziecku podczas korzystania z Sieci.

III Przeciwdziałanie problemowi

„Internet to nowe narzędzie komunikacji społecznej i jako takie znajduje szerokie zastosowanie w wielu obszarach – od edukacji i nauki po biznes i kontakty prywatne. Choć sieć nie jest już nowinką technologiczną, a w Polsce korzysta z niego ponad 15 milionów osób, to wiedza na temat podstawowych zasad bezpieczeństwa wciąż nie jest powszechna. Dotyczy to zarówno korzystania z witryn i usług w sieci jak i tworzenia tego typu rozwiązań. Podstawowe aspekty związane z zapewnieniem komfortu korzystania z internetu są w moim odczuciu związane z ochroną prywatności, w tym ochroną korespondencji, bezpieczeństwem finansowym oraz przestrzeganiem obowiązujących przepisów prawa.

Niewielkie doświadczenie internautów wynikające z krótkiego stażu sieciowego sprawia, że użytkownicy nie są jeszcze wystarczająco wyczuleni w zakresie ochrony prywatności. Internet to powszechnie dostępna sieć informacyjna. Należy zatem korzystać z jego możliwości z rozwagą. Publikowanie w sieci informacji o charakterze intymnym czy po prostu osobistym może prowadzić do naruszeń prywatności. Problem ten dotyczy zwłaszcza dzieci i młodzieży surfującej, coraz częściej bez ograniczeń, w Internecie. Myślę, że nie do przecenienia jest konieczność edukacji w tym zakresie (szkoła, rodzice). Z drugiej strony dzięki narzędziom i rozwiązaniom technicznym służącym do budowy witryn sieciowych istnieje szereg możliwości przynajmniej w podstawowy sposób zabezpieczających najmłodszych przed publikowaniem danych wrażliwych. Moim zdaniem stosowanie takich mechanizmów jest obowiązkiem każdego odpowiedzialnego twórcy stron internetowych. Podstawowymi rozwiązaniami podnoszącymi efektywność ochrony osób niepełnoletnich są przede wszystkim: weryfikacja deklarowanego wieku, analiza aktywności i wypowiedzi udzielanych na forach internetowych, weryfikacja numerów IP komputerów użytkowników oraz uczulanie społeczności na wszelkiego rodzaju próby wyłudzeń informacji wrażliwych – takich jak e-mail czy telefon. W tym zakresie samoregulacja i powiadomienia użytkowników, którzy dostrzegają niepokojące sygnały i zgłaszają je administratorom są nie do przecenienia. Uważam, że strony skierowane w swoim założeniu do osób niepełnoletnich powinny stosować podwyższone standardy bezpieczeństwa i ochrony niż te wynikające ze stosownych przepisów.

Kodeksy dobrych praktyk oraz standardy rynkowe są przykładem rosnącej świadomości wspomnianych zagrożeń i w moim odczuciu przyczyniają się do wzrostu bezpieczeństwa w Internecie. Jednak należy pamiętać, że żaden dokument nie zastąpi odpowiedzialności przedsiębiorców kierujących swoje serwisy do dzieci i młodzieży. Dlatego presja rynkowa, płynąca zarówno ze strony użytkowników, mediów jak i organizacji branżowych może skutecznie podwyższyć standard rozwiązań stosowanych w tym zakresie."

Dominik Kaznowski

Przewodniczący Rady Nadzorczej IAB Polska

Skuteczne przeciwdziałanie zagrożeniom dzieci w Internecie wymaga szeregu kompleksowych działań w obszarze prawa, edukacji i technologii.

Przepisy prawne uwzględniać muszą zmieniające się realia związane z postępem technicznym i dostrzegać nowe formy przestępstw w cyberprzestrzeni, których ofiarami padają dzieci. Rozwiązania legislacyjne musza też dawać organom ścigania i wymiaru sprawiedliwości narzędzia, pozwalające na skuteczne przeciwdziałanie przestępczości wobec najmłodszych użytkowników Internetu.

Nawet najlepsze przepisy prawne nie wyeliminują w pełni sytuacji, stanowiących dla dzieci zagrożenie *on-line*. Niezwykle ważnym elementem systemowego zapobiegania zagrożeniom dla dzieci w Internecie staje się więc edukacja. Prowadzone na różnych poziomach działania profilaktyczne powinny być adresowane przede wszystkim do najmłodszych, ale również do rodziców i profesjonalistów. Celem takich działań powinno być uświadomienie ich odbiorcom zakresu zagrożeń występujących w Sieci, sposobów ich unikania i zapobiegania tym zagrożeniom oraz sposobów reagowania na niebezpieczne zdarzenia w Internecie.

Podniesienie poziomu bezpieczeństwa dzieci *on-line* zależy również od dostawców usług internetowych i producentów sprzętu elektronicznego oraz oprogramowania. Rozwiązania technologiczne w dużym stopniu wpływać mogą na poziom bezpieczeństwa dzieci *on-line* i mogą stanowić dla opiekunów młodych internautów pomoc w czuwaniu nad ich bezpieczeństwem.

3.1 Prawo

Prawo międzynarodowe

Fundamentalnym międzynarodowym aktem prawnym dotyczącym ochrony dzieci przed wszelkimi formami krzywdzenia jest **Konwencja ONZ o Prawach Dziecka**.

Artykuł 34 Konwencji poświęcony został kwestiom związanym z wykorzystywaniem seksualnym, dzieci i rządy krajów które ją ratyfikowały zobowiązały się do podejmowania wszelkich działań w celu przeciwdziałania:

a) nakłanianiu lub zmuszaniu dziecka do jakichkolwiek nielegalnych działań seksualnych;
b) wykorzystywaniu dzieci do prostytucji lub innych nielegalnych praktyk seksualnych;
c) wykorzystywaniu dzieci w pornograficznych przedstawieniach i materiałach.

Zapisy Konwencji, wraz z przytoczonym wyżej artykułem opracowywane pod koniec lat ’80 zeszłego stulecia i nie uwzględniały specyfiki Internetu ale w oczywisty sposób stosują się do nowych

form wykorzystywania seksualnego dzieci. Tym niemniej ustawodawcy działający w imieniu ONZ uznali za konieczne dostosowanie zapisów Konwencji do zmieniającej się rzeczywistości. **Protokół Opcjonalny do Konwencji o Prawach Dziecka** z 25 maja 2000 r. uwzględniając *rosnącą dostępność pornografii dziecięcej w Internecie*[12], uściślił kwestie związane z pornografią dziecięcą i zobowiązał strony, które go ratyfikowały, do penalizacji produkcji, dystrybucji, obrotu i posiadania pornografii dziecięcej.

Ogólne zapisy Konwencji o Prawach dziecka odnieść można również do innych form krzywdzenia dzieci w Internecie, szczególnie związanych ze zjawiskiem cyberprzemocy (Podlewska, Mierzejewska 2008). Do kwestii zniesławiania, znieważania oraz naruszania wizerunku dzieci w Sieci odnieść można artykuł 8 Konwencji:

1. Państwa-Strony podejmują działania mające na celu poszanowanie prawa dziecka do zachowania jego tożsamości, w tym obywatelstwa, nazwiska, stosunków rodzinnych, zgodnych z prawem, z wyłączeniem bezprawnych ingerencji.

2. W przypadku, gdy dziecko zostało bezprawnie pozbawione części lub wszystkich elementów swojej tożsamości, Państwa-Strony okażą właściwą pomoc i ochronę w celu jak najszybszego przywrócenia jego tożsamości.

Z kolei do problemu naruszania prywatności dziecka, związanego często z włamaniami na internetowe profile i konta odnosi się artykuł 16 Konwencji:

1. Żadne dziecko nie będzie podlegało arbitralnej lub bezprawnej ingerencji w sferę jego życia prywatnego, rodzinnego lub domowego czy w korespondencję ani bezprawnym zamachom na jego honor i reputację.

2. Dziecko ma prawo do ochrony prawnej przeciwko tego rodzaju ingerencji lub zamachom.

Problem gróźb, który w rzeczywistości internetowej pojawia się zarówno w przypadkach cyberprzemocy jaki i uwodzenia dzieci, odnieść można do artykułu 19 Konwencji:

Państwa-Strony będą podejmowały wszelkie właściwe kroki w dziedzinie ustawodawczej, administracyjnej, społecznej oraz wychowawczej dla ochrony dziecka przed wszelkimi formami przemocy fizycznej bądź psychicznej, krzywdy lub zaniedbania bądź złego traktowania lub wyzysku, w tym wykorzystywania w celach

[12] Zapis Preambuły Protokołu.

seksualnych, dzieci pozostających pod opieką rodzica(ów), opiekuna(ów) prawnego(ych) lub innej osoby sprawującej opiekę nad dzieckiem.

Kwestie związane z problemem wykorzystywania seksualnego dzieci w Internecie reguluje też uchwalona przez Radę Europy w listopadzie 2001 r**. Międzynarodowa Konwencja o Cyberprzestępczości**. Dokument ten jest w dużej mierze konsekwencją ustaleń zapisanych w dokumentach ONZ[13] i zaleca (artykuł 9) państwom, które go ratyfikują, podjęcie wszelkich środków dla uznania w ich wewnętrznym prawie za przestępstwa:

a) produkowanie pornografii dziecięcej dla celów jej rozpowszechniania za pomocą systemu informatycznego;
b) oferowanie lub udostępniania pornografii dziecięcej za pomocą systemu informatycznego;
c) rozpowszechnianie lub transmitowanie pornografii dziecięcej za pomocą systemu informatycznego;
d) pozyskiwanie pornografii dziecięcej za pomocą systemu informatycznego dla siebie lub innej osoby;
e) posiadanie pornografii dziecięcej w ramach systemu informatycznego lub na środkach do przechowywania danych informatycznych.

Wszystkie wyżej przytaczane dokumenty międzynarodowe zalecają ustalenie granicy wieku ochrony dzieci przed krzywdzeniem dzieci na poziomie 18 lat.

Przepisy krajowe

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

Sytuacja tak miała długi czas miejsce w odniesieniu do zapisów polskiego kodeksu karnego odnośnie prawnego zakazu posiadania pornografii dziecięcej. Przepis zakazujący posiadania materiałów pornograficznych z udziałem dzieci, co w praktyce sprowadza się również do zakazu przeglądania i ściągania takich materiałów przy użyciu Internetu, wprowadzony został dopiero ustawą z 18 marca 2004 r. Od tego czasu artykuł 202 KK, który znajduje zastosowanie w przypadkach **narzucania dzieciom w Internecie kontaktu z treściami pornograficznymi** oraz w sytuacjach

[13] Patrz: Preambuła Konwencji

utrwalania, sprowadzania, przechowywania oraz posiadania materiałów pornograficznych z udziałem dzieci zyskał brzmienie:

§ 1. 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.
§ 2. 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.
§ 3. Kto w celu rozpowszechniania produkuje, utrwala lub sprowadza albo rozpowszechnia lub publicznie prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 4. Kto utrwala, sprowadza, przechowuje lub posiada treści pornograficzne z udziałem małoletniego poniżej lat 15, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 5. Sąd może orzec przepadek narzędzi lub innych przedmiotów, które służyły lub były przeznaczone do popełnienia przestępstw określonych w § 1–4, chociażby nie stanowiły własności sprawcy.

Kwestie **uwodzenia dzieci** za pośrednictwem internetowych serwisów komunikacyjnych nie są wprost podejmowane przez polskie przepisy prawne. Po części reguluje je artykuł 200 kk,:

Art. 200 kk
§ 1 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. użyty w nim termin „doprowadza" jest jednak na tyle nie precyzyjny, że pozostawia pole do różnych interpretacji (Adamski 2004). Niewątpliwie dowiedzenie na podstawie tego przepisu winy osobie uwodzącej dziecko w Internecie jest rzeczą niezmiernie problematyczną.

W przypadkach zagrożeń, składających się na problem cyberprzemocy, polskie prawo nie zapewnia w pełni skutecznej ochrony, mimo to wykorzystując istniejące regulacje prawne można w pewnym zakresie chronić małoletnie ofiary przemocy w Internecie Ze względu na różnorodność form

zjawiska cyberprzemocy nie zawsze kwestie te regulowane są w kodeksie karnym. W niektórych przypadkach jedynym sposobem ochrony prawnej jest droga cywilna czyli droga roszczeń odszkodowawczych (Podlewska, Mierzejewska 2008). Poniżej zaprezentowane przepisy prawne zapisane w kodeksie karnym, kodeksie cywilnym oraz kodeksie wykroczeń znajdują zastosowanie w odpowiednich obszarach zjawiska cyberprzemocy.

Naruszenie wizerunku

Art. 23 kc

Dobra osobiste człowieka, jak w szczególności zdrowie, wolność, cześć, swoboda sumienia, nazwisko lub pseudonim, wizerunek, tajemnica korespondencji, nietykalność mieszkania, twórczość naukowa, artystyczna, wynalazcza i racjonalizatorska, pozostają pod ochroną prawa cywilnego niezależnie od ochrony przewidzianej w innych przepisach.

Art. 24. kc

§ 1.Ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba, że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków, w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego lub zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.
§ 2. Jeżeli wskutek naruszenia dobra osobistego została wyrządzona szkoda majątkowa, poszkodowany może żądać jej naprawienia na zasadach ogólnych.
§ 3. Przepisy powyższe nie uchybiają uprawnieniom przewidzianym w innych przepisach, w szczególności w prawie autorskim oraz w prawie wynalazczym.

Naruszenie czci (zniesławienie, znieważenie)

Art. 212 kk

§ 1. Kto pomawia inną osobę, grupę osób, instytucję, osobę prawną lub jednostkę organizacyjną nie mającą osobowości prawnej o takie postępowanie lub właściwości, które mogą poniżyć ją w opinii publicznej lub narazić na utratę zaufania potrzebnego dla danego stanowiska, zawodu lub rodzaju działalności,
podlega grzywnie, karze ograniczenia albo pozbawienia wolności do roku.

§ 2. Jeżeli sprawca dopuszcza się czynu określonego w § 1 za pomocą środków masowego komunikowania,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 3. W razie skazania za przestępstwo określone w § 1 lub 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.
§ 4. Ściganie przestępstwa określonego w § 1 lub 2 odbywa się z oskarżenia prywatnego.

Art. 216 kk

§ 1. Kto znieważa inną osobę w jej obecności albo choćby pod jej nieobecność, lecz publicznie lub w zamiarze, aby zniewaga do osoby tej dotarła,
podlega grzywnie albo karze ograniczenia wolności.
§ 2. Kto znieważa inną osobę za pomocą środków masowego komunikowania,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
§ 3. Jeżeli zniewagę wywołało wyzywające zachowanie się pokrzywdzonego albo jeżeli pokrzywdzony odpowiedział naruszeniem nietykalności cielesnej lub zniewagą wzajemną, sąd może odstąpić od wymierzenia kary.
§ 4. W razie skazania za przestępstwo określone w § 2 sąd może orzec nawiązkę na rzecz pokrzywdzonego, Polskiego Czerwonego Krzyża albo na inny cel społeczny wskazany przez pokrzywdzonego.
§ 5. Ściganie odbywa się z oskarżenia prywatnego.

Włamania

Art. 267 kk

§ 1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie,
podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
§ 2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.
§ 3. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1 lub 2 ujawnia innej osobie.
§ 4. Ściganie przestępstwa określonego w § 1-3 następuje na wniosek pokrzywdzonego.

Art. 268a. kk

§ 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych,
podlega karze pozbawienia wolności do lat 3.
§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową,
podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego.

Groźby

Art. 190 kk

§ 1. Kto grozi innej osobie popełnieniem przestępstwa na jej szkodę lub szkodę osoby najbliższej, jeżeli groźba wzbudza w zagrożonym uzasadnioną obawę, że będzie spełniona, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.§ 2. Ściganie następuje na wniosek pokrzywdzonego.

Art. 191 kk

§ 1. Kto stosuje przemoc wobec osoby lub groźbę bezprawną w celu zmuszenia innej osoby do określonego działania, zaniechania lub znoszenia, podlega karze pozbawienia wolności do lat 3.
§ 2. Jeżeli sprawca działa w sposób określony w § 1 w celu wymuszenia zwrotu wierzytelności, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

Nękanie

Art. 107 kw

Kto w celu dokuczenia innej osobie złośliwie wprowadza ją w błąd lub w inny sposób złośliwie niepokoi, podlega karze ograniczenia wolności, grzywny do 1.500 zł albo karze nagany.

Wulgaryzmy

Art. 141 kw

Kto w miejscu publicznym umieszcza nieprzyzwoite ogłoszenie, napis lub rysunek albo używa słów nieprzyzwoitych, podlega karze ograniczenia wolności, grzywny do 1.500 zł albo karze nagany.

Postulowane kierunki zmian:

Środowisko profesjonalistów w toku dyskusji na tematy związane z pożądanymi kierunkami zmian w obrębie regulacji prawnych, dotyczących bezpieczeństwa dzieci w Internecie wskazuje m.in. na następujące kwestie:[14]

1. Konieczność prawnego uregulowania możliwości stosowania przez policję narzędzia prowokacji w zakresie spraw dotyczących przestępstw seksualnych wobec dzieci, w tym szczególnie przestępstw z wykorzystaniem Internetu. Zmiany w prawie powinny uczynić z prowokacji tak skuteczne narzędzie do walki z pedofilią, jakim jest ono w innych krajach Europy i w USA.[15]

2. Potrzebę regulacji prawnych w zakresie skutecznego zabezpieczenia dostępu dzieci do reklam, zawierających brutalne sceny przemocy i inne szkodliwe treści, w szczególności zaś tych, które przypominając zwykłą stronę internetową, ukrywają perswazyjny i/lub reklamowy charakter komunikatu.

3. Konieczność edukacji sędziów w zakresie standardów orzecznictwa i przepisów prawa dotyczących przestępstw przy użyciu nowoczesnych technologii lub w odniesieniu do dzieci.

4. Zmiana prawa umożliwiająca karanie tzw. wirtualnej pornografii dziecięcej, gdzie osoba dziecka jest zastąpiona sugestywną i jednoznaczną grafiką lub zmodyfikowanym zdjęciem.

5. Zmiana i ujednolicenie wieku małoletniego z 15 na 18 lat – czyli podwyższenie wieku specjalnej ochrony (art. 200 KK, art.202 KK);

6. Przyjęcie porozumienia finansowego banków – dla realizowania blokady transakcji finansowych pochodzących ze stron zawierających pornografię dziecięcą

7. Odpowiedzialność karna wg „zasady państwa pochodzenia" oraz „zasady państwa odbioru"

[14] Wnioski z panelu dyskusyjnego z udziałem profesjonalistów z zakresu prawa zorganizowanego w ramach seminarium „Bezpieczeństwo dzieci w Internecie" (organizacja: FDN, Microsoft, Warszawa 10 kwietnia 2008). Postulaty przytoczone za wydawnictwem pokonferencyjnym.

[15] we wrześniu 2008 roku MSWIA zaproponowała kompleksowe zmiany w przepisach prawnych, które mają m.in. zapewnić policji skuteczne stosowanie prowokacji w przypadkach pedofilii w Sieci

3.2 Edukacja

Skuteczna edukacja na rzecz bezpieczeństwa dzieci w Internecie prowadzona musi być kompleksowo uwzględniając spektrum zjawisk uznanych za zagrażające dzieciom i korzystać musi z tradycyjnych oraz najnowszych form edukacyjnych. Projekty edukacyjne powinny uwzględniać dynamikę rozwoju mediów elektronicznych i bazować na najnowszych ustaleniach teoretycznych i empirycznych pokazujących specyfikę zagrożeń dla dzieci w Internecie.

Odbiorcy i cel

Odbiorcami propozycji edukacyjnych powinni być najmłodsi użytkownicy Internetu, jak również ich opiekunowie. Ważną grupą odbiorców działań edukacyjnych muszą być również profesjonaliści, pracujący z dziećmi.

Edukacja najmłodszych użytkowników Internetu stawiać sobie musi za cel przede wszystkim:

- Zapoznanie dzieci i młodzieży ze specyfiką zagrożeń w Sieci
- Nauczenie odbiorców korzystania z Sieci w sposób pozwalający na uniknięcie zagrożeń
- Nauczenie młodych internautów reagowania w sytuacjach zagrożenia

Skuteczna edukacja rodziców i profesjonalistów musi w pierwszym rzędzie uświadomić im jak ważną rolę pełną w zakresie zapewnienia bezpieczeństwa dzieci *on-line*. Skuteczne działania wobec tej grupy musza się też koncentrować na uświadomieniu części odbiorców, że niski poziom znajomości mediów elektronicznych nie jest bezwzględną przeszkodą w realizowaniu działań na rzecz bezpieczeństwa młodych internautów oraz nie zwalnia ich z odpowiedzialności za bezpieczeństwo dzieci. Ponadto celami edukacji tej grupy odbiorców jest przekazanie im wiedzy w zakresie:

- specyfiki mediów elektronicznych
- specyfiki zagrożeń związanych z korzystaniem z Internetu przez dzieci i młodzież
- zasad bezpiecznego korzystania z Internetu przez najmłodszych
- sposobów na zapewnienie dzieciom bezpieczeństwa *on-line*
- sposobów przekazywania najmłodszym wiedzy dotyczącej bezpieczeństwa w Sieci
- procedur reagowania w sytuacji zagrożenia

Formy i realizatorzy

W zależności od tematyki i skali realizowanych działań profilaktycznych, ich odbiorców oraz możliwości technicznych ich realizatorów działania te mogą być realizowane równymi środkami:

- kampanie społeczne

Kampanie społeczne to zwykle kompleksowe działania profilaktyczne realizowane na dużą skalę i adresowane do licznej grupy odbiorców. Treść przekazów medialnych przygotowywanych na potrzeby kampanii, prezentowanych w postaci reklamy prasowej, telewizyjnej, radiowej, internetowej, czy zewnętrznej (outdoor), ogranicza się za zwyczaj do krótkiego komunikatu sygnalizującego występowanie problemu i postulującego zapobieganie mu. Komunikaty medialne kampanii społecznych za zwyczaj kierują odbiorców, najczęściej za pośrednictwem serwisu internetowego, do pogłębionej wiedzy na temat podejmowanego problemu oraz propozycji edukacyjnych z nim związanych. Materiały edukacyjne kampanii często dystrybuowane są też w postaci wysokonakładowych materiałów drukowanych, takich jak ulotki, broszury, czy plakaty.

Realizatorami kampanii społecznych podejmujących zagadnienia związane z bezpieczeństwem dzieci *on-line* są za zwyczaj organizacje pozarządowe, firmy z branży IT, instytucje rządowe. W Polsce dużą rozpoznawalnością cieszy się kampania „Dziecko w Sieci", podejmująca w swoich kolejnych odsłonach kwestie niebezpiecznych kontaktów *on-line* („Nigdy nie wiadomo, kto jest po drugiej stronie), niebezpiecznych treści w Sieci („Internet to okno na świat. Cały świat") oraz czyberprzemocy (Powiedź stop cyberprzemocy).[16]

- zajęcia edukacyjne

Problematyka bezpieczeństwa dzieci w Internecie powinna być stałym elementem programów nauczania w szkołach, szczególnie podstawowych i gimnazjalnych, których uczniowie zaczynają dopiero swoją przygodę z Internetem i największym stopniu narażeni są na zagrożenia *on-line***.** Szkoły, które zdecydowały się włączyć tą problematykę do programu nauczania, lub nauczyciele który poruszają tą tematykę z własnej inicjatywy, tworzą autorskie programy zajęć lub korzystają ze propozycji edukacyjnych opracowanych zewnętrznie i udostępnianych w formie drukowanej lub elektronicznej. Najbogatsza oferta edukacyjna poświęcona bezpieczeństwu dzieci

[16] Badania opinii publicznej po kolejnych medialnych odsłonach kampanii dziecko w Sieci wskazują na rozpoznawalność kampanii na poziomie ponad 70%! (Gemius 2007, OBOB 2008)

on-line udostępniana jest w ramach kampanii „Dziecko Sieci" w postaci zestawów edukacyjnych (książki, płyty CD) oraz *on-line* z poziomu serwisu www.dzieckowsieci.pl (elektroniczne wersje scenariuszy, materiały multimedialne, kursy e-learning)

Wzmiankowane wyżej materiały edukacyjne są ofertą głównie dla szkół jednak znajdują zastosowanie również w innych placówkach pracujących z dziećmi, jak domy kultury, ogniska wychowawcze itp. Realizatorami działań profilaktycznych oprócz nauczycieli mogą być studenci, wychowawcy, wolontariusze.[17] Materiały edukacyjne mogą być również źródłem wiedzy i inspiracją dla rodziców aktywnie dbających o bezpieczeństwo swoich dzieci w Sieci.

Nowa podstawa programowa opracowana przez Ministerstwo Edukacji Narodowej, która obowiązywać będzie od roku szkolnego 2009/2010 , w dużo większym niż dotychczas stopniu, podejmuje tematykę bezpieczeństwa dzieci w Internecie . Należy się więc spodziewać, ze w najbliższym czasie liczba propozycji edukacyjnych na ten temat na polskim rynku istotnie wzrośnie.

- serwisy edukacyjne, wydawnictwa

Podejmowanie przez dorosłych działań na rzecz bezpieczeństwa dzieci w Internecie, nie wymaga co prawda fachowej wiedzy dotyczącej mediów elektronicznych, jednak podstawowe wiadomości na ten temat uzupełnione informacjami o specyfice zagrożeń i zalecanych działaniach profilaktycznych są niewątpliwie wskazane. Informacje takie znaleźć można w nielicznych serwisach internetowych i publikacjach o tejże tematyce[18].

W Sieci znaleźć można również serwisy poświęcone bezpieczeństwu dzieci *on-line* adresowane bezpośrednio do dzieci i młodzieży, np.: www.dzieckowsieci.pl, www.bezpiecznyinternet.org, www.saferinternet.pl. Takie strony mogą być polecane dzieciom przez rodziców i nauczycieli. Można je również wykorzystać podczas zajęć edukacyjnych.[19]

Wartym uwagi jest serwis www.sieciaki.pl w pełni poświęcony bezpieczeństwu dzieci w Internecie. Fabuła serwisu oparta jest na konflikcie pozytywnych bohaterów – sieciaków - z czarnymi charakterami będącymi uosobieniem zagrożeń czyhających na dzieci w Internecie -sieciuchami. W serwisie znaleźć można kreskówki, teledyski, filmy i inne materiały multimedialne związane z bezpieczeństwem *on-line.* Zarejestrowani użytkownicy portalu otrzymują codziennie informacje związane z bezpiecznym i efektywnym korzystaniem z Sieci oraz biorą udział w licznych konkursach z atrakcyjnymi nagrodami.

[17] Działania edukacyjne w szkołach coraz częściej realizowane są woluntarystycznie przez pracowników dużych firm. Zajęcia poświęcone bezpieczeństwu dzieci *on-line* prowadzone są w ramach wolontariatu pracowniczego np. przez pracowników Telekomunikacji Polskiej.

[18] W polskich zasobach Internetu znaleźć można serwisy: www.sieciaki.pl, www.przedszkolaki.sieciaki.pl

Autorzy serwisu Sieciaki.pl pomyśleli też o najmłodszych dzieciach. Pod adresem www.przedszkolaki.sieciaki.pl dzieci w wieku przedszkolnym Wartym uwagi jest serwis www.sieciaki.pl w pełni poświęcony bezpieczeństwu dzieci w znajdą atrakcyjną graficznie stronę ukierunkowaną na podstawowe zagadnienia związane z komputerem i Internetem.

Przykładem serwisu edukacyjnego poświęconego bezpieczeństwu dzieci *on-line* może być też dzieci.wp.pl. Na początku 2008 roku przeprowadzono tam akcję „Bądź bezpieczny w sieci". Za pomocą pomocą bajkowych postaci dzieci poznają pięć podstawowych zasad bezpiecznego korzystania z Internetu. Dowiadują się m.in. tego, że wiele stron WWW nie jest przeznaczonych dla nich, że nie mogą przekazywać nieznajomym, za pośrednictwem Internetu, żadnych informacji o sobie i że bez zgody dorosłych nie powinny wysyłać przez sieć swoich zdjęć ani innych prywatnych materiałów. W ramach akcji twórcy serwisu zachęcają również do tego, aby o wszystkich krokach dziecka w Internecie wiedzieli rodzice, by to oni decydowali o witrynach, które dzieci mogą oglądać i towarzyszyli im we wszystkich „internetowych wędrówkach".

Postulowane kierunki zmian:

Specjaliści z dzieciny edukacji wskazują na następujące kwestie związane z poprawą systemu edukacji w zakresie tematyki bezpieczeństwa dzieci *on-line*:

1. Konieczność zapewnienia przez szkołę bardziej kompleksowej, nowatorskiej i zintegrowanej edukacji, dostarczania, oprócz wiedzy, także umiejętności, w tym szczególnie tych społecznych.
2. Konieczność interwencji w podstawę programową, być może opracowanie poradnika dla dyrektorów i nauczycieli dotyczącego bezpieczeństwa jako elementu nauczania i wychowania w szkole. Bezpieczeństwo dzieci w Internecie powinno być prezentowanie w szerszym kontekście bezpieczeństwa w ogóle, w odniesieniu do zachowań agresywnych, przestrzegania prawa, ochrony przed używkami, ale także w kontekście propagowania otwartości na odmienność, tolerancji, kształtowania zachowań prospołecznych, wrażliwości na krzywdę i eliminowania obojętności / bierności

    a. Praca nad wykształceniem u dzieci i młodzieży nawyku bezpiecznego korzystania z Internetu i technologii powinna być zwieńczeniem edukacji z zakresu komunikacji interpersonalnej, asertywności, umiejętności radzenia sobie ze stresem, zastępowania agresji

3. Włączenie rodziców w działalność szkoły, aktywizowanie ich. Zachęcanie do interesowania się tym, co dzieci robią w szkole i poza nią, stworzenie bardziej wydajnych możliwości wyrażenia swojego zdania w tym zakresie.

    a. Troska o pomoc rodzicom w kształtowaniu prawidłowych i trwałych więzów rodzinnych, przekazywanie zasad i prawidłową, efektywną socjalizację w rodzinie.

4. Konieczność masowego kształcenia nauczycieli w zakresie korzystania z nowoczesnych technologii w edukacji, komunikowania się z uczniami i rodzicami w ten sposób, kształtowania nawyków ich bezpiecznego użytkowania.

5. Konieczność edukacji dzieci i młodzieży w związku z rozpowszechnianiem się sklepów *on-line* i robieniem zakupów przez Internet.

3.3 Technologia

Zagrożenia związane z Internetem są pośrednio efektem intensywnego rozwoju technologii. Nowe media w nieodpowiednich rękach wykorzystywane są do działalności przestępczej, kierowanej również przeciwko dzieciom. Tym niemniej rozwiązania technologiczne zarówno sprzętowe (hardware) jak i programowe (software) są ważnym elementem zapobiegania zagrożeniom dla dzieci w Internecie. W tym zakresie ważna jest również postawa firm, które kreują lub wykorzystują technologię na potrzeby usług świadczonych z użyciem Internetu. Skuteczne działania na rzecz bezpieczeństwa dzieci w Internecie wymagają od nich świadomości zagrożeń, poczucia odpowiedzialności za bezpieczeństwo najmłodszych użytkowników Sieci oraz współpracy w tym zakresie z podmiotami z branży edukacyjnej i prawnej.

Olgierd Cygan – CEO/Managing Partner agencji interaktywnej Digital One, która wielokrotnie tworzyła serwisy skierowane do dzieci i młodzieży, uważa że podstawowym kryterium podczas pracy nad takiego rodzaju realizacją jest wyjątkowa ostrożność w doborze treści i środków- *„Bazując na naszym wieloletnim doświadczeniu w realizacji projektów skierowanych do dzieci i młodzieży (Klub Mamby dla firmy Storck, czy Bądź MAX na Fotka.pl dla firmy Pepsi-Cola General Bottlers Poland), możemy wysunąć tezę, iż w odróżnieniu od projektów skierowanych do dorosłych odbiorców, projekty dla dzieci wymagają szczególnej uwagi, ostrożności oraz dokładności w przygotowaniu materiałów. Każdy z etapów*

planowania projektu należy przygotowywać z ogromna rozwagą, począwszy od tworzenia założeń merytorycznych, doboru rozwiązań i narzędzi, poprzez realizację oraz późniejsze utrzymanie projektu. Nie jest to wyłącznie zwrócenie uwagi na używane słownictwo, zastosowaną kolorystykę, wielkość czcionek czy milusińskie postacie.

Warto jeszcze pamiętać o tym, co jest na drugim planie / pod spodem projektu,

czyli powinniśmy mieć na uwadze, aby:

- cały projekt był maksymalnie transparentny

- rodzice mieli pełen wgląd w założenia projektu

- rodzice wiedzieli, kto za tym stoi, z kim można się skontaktować

- zasady bezpieczeństwa, wykorzystywania danych kontaktowych, komunikacji były jasne i zrozumiałe

- rodzice byli powiadamiani o korespondencji, która jest kierowana do ich dzieci, nie wspominając ze prawnie musza wyrazić na nią zgodę

Ponadto bardzo sensytywnym tematem jest udział w projekcie firm trzecich, coopromocje lub ew. inne działania łączone (w projektach dla dorosłych jest to normalne, tutaj niekoniecznie)

W dobie wzmożonej komunikacji miedzy internautami trzeba również pod uwagę brać fakt, że wszelkie narzędzia typu komunikatory, czaty, fora, etc, do których dostęp maja wszyscy internauci, są w przypadku serwisów dziecięcych potencjalnie bardzo dużym niebezpieczeństwem. Dają bowiem możliwość podszywania się pod dzieci osobom o złych intencjach, co nawet przy podwyższonym poziomie monitoringu ze strony administratorów, nie pozwala wykluczyć zagrożenia, jakim są niebezpieczne treści.

Wiele firm z założenia blokuje wszelkie możliwości interakcji pomiędzy użytkownikami swojego serwisu, aby nie dopuścić do tego typu potencjalnej sytuacji, która jest de facto kryzysem, silnie uderzającym w markę.

Należy przyjąć, że każdy poziom zabezpieczeń jest do obejścia i niezależnie od tego, jak to ustawimy zawsze może znaleźć się ktoś, kto zarejestruje się w systemie i złamie ochronę.

Mimo to należy bezwzględnie pamiętać o tym, że poziom zabezpieczeń musi być trzykrotnie większy niż w klasycznych projektach. Rekomendujemy także ustawianie stałego monitoringu aktywności internautów w oparciu o administratorów po naszej stronie, którzy starają się systematycznie eliminować dziwne i niestandardowe zachowania użytkowników.

Kolejnym zabezpieczeniem może być także ustawienie filtrów monitorujących wybrane frazy w korespondencji, tak aby wyłapywać niebezpieczne treści.

Można pokusić się o tezę, iż w pogoni za nowinkami czasami niechcący można narazić małoletniego odbiorcę na niebezpieczeństwo. Dokładnie nie wiadomo, jaki impakt mają owe nowości na codzienne funkcjonowanie websiteu i jego użytkowników, gdyż są swego rodzaju eksperymentem, na który, w przypadku serwisów dla

dzieci, po prostu nas nie stać, ponieważ niesie ze sobą zbyt duże ryzyko, a ryzyko to element niepożądany przy tej grupie docelowej.
Należy uważać także z nowinkami po stronie mediów - reklama w serwisach społecznościowych, profile w serwisach społecznościowych, etc. - to rzeczy, które jeszcze nie są dobrze poznane i nie wiemy z konkretnie jakim ryzykiem wiążą się.
Reasumując: wyjątkowo ostrożne, a nawet zachowawcze działanie w trakcie pracy nad realizacją projektów skierowanych do dzieci i młodzieży, to cena jaką musi zapłacić każda profesjonalna agencja interaktywna."

Technologia znajduje zastosowanie w działaniach na rzecz bezpieczeństwa dzieci głownie w następujących obszarach:

- wsparcie dorosłych w zapewnianiu bezpieczeństwa młodym internautom
- profilaktyka zagrożeń podejmowana przez dostawców usług
- wsparcie organów ścigania w zwalczaniu przestępczości wobec dzieci

Ważną rolę odgrywają także Administratorzy Sieci, do których kierowane są sygnały dotyczące nadużyć. Zdaniem Marka Dudka, kierownika Dyżurnetu, „zwiększa się świadomość odpowiedzialności społecznej. Administratorom zależy na tym, aby działać zgodnie z prawem oraz mają na uwadze dobro dzieci, przykładem jest Google do którego należy YouTube.com czy blogi na blogspot*.com. Ktoś powie, że na serwisach ze śmiesznymi filmikami, z których bardzo chętnie korzysta młodzież, ostrzeżenia o treściach dozwolonych od lat 18 są zupełnie niepotrzebne. Nie ma nic prostszego niż zaznaczenie „tak, mam 18 lat". Owszem jest łatwo, ale takie ostrzeżenie przygotowuje nas, że za chwilę mogę zobaczyć treści, które mogą być trudne, których mogę nie zrozumieć, których nie powinienem oglądać. Takie ostrzeżenia są również łatwiejsze do wyłapania i zablokowania całej strony przez programy filtrujące. Są oczywiście administratorzy, którzy za wszelką cenę chcą przyciągnąć użytkownika i nie sa zainteresowani ich blokowaniem. Błędnie interpretując prawo zasłaniają się tym, że nie są odpowiedzialni za to, co ich użytkownicy umieszczają w serwisach. A prawo reguluje to w ten sposób, że i owszem nie mają obowiązku wiedzieć co jest w takim serwisie, ale po zgłoszeniu informacji o nielegalnej stronie przejmują na siebie odpowiedzialność za publikowane treści. Jest to zapisane w art. 14 Ustawy o Świadczeniu Usług Drogą Elektroniczną."*

3.4 Wsparcie dorosłych w zapewnianiu bezpieczeństwa młodym internautom

W działaniach rodziców, czy szkoły na rzecz bezpieczeństwa dzieci w Internecie pierwszorzędne zastosowanie znajduje niewątpliwie edukacja. Nic nie zastąpi rzeczowej rozmowy na temat zagrożeń, ustalenia zasad korzystania z Internetu i sposobów reagowania w niebezpiecznych sytuacjach. Rozwiązania technologiczne, takie jak oprogramowanie filtrujące, czy programy umożliwiające szersza kontrolę w zakresie dostępu dzieci do zasobów Internetu mogą jednak być pomocne.

Oprogramowanie filtrujące od kilkunastu już lat produkowane jest w celu zabezpieczania dostępu dzieci do niepożądanych zasobów Internetu. Wiodące polskojęzyczne programy filtrujące to. Beniamin, Cenzor, Motyl, Ochraniacz, Opiekun Dziecka w Internecie, Strażnik Ucznia,. Weblock, X Guard II.[20] Większość tego typu oprogramowania dystrybuowana jest komercyjnie, nieliczne programy dostępne są bezpłatnie.[21]

Zasadność stosowania filtrów jest dyskusyjna. Część środowiska profesjonalistów, zajmujących się bezpieczeństwem dzieci, uznaje, że używanie takich programów przez rodziców rodzi u nich błędne przekonanie o bezpieczeństwie, podczas gdy programy takie znajdują zastosowane jedynie w odniesieniu do jednej z wielu kategorii zagrożeń dzieci *online*. Ponadto zwraca się uwagę na niedoskonałość programów filtrujących polegającą na nie wykrywaniu wszystkich niebezpiecznych treści przy jednoczesnym blokowaniu stron bezpiecznych i wartościowych.

Ograniczenia oprogramowania filtrującego potwierdza analiza wiodących polskich programów wykonana w 2007 roku przez Naukową i Akademicką Sieć Komputerową przy udziale specjalistów z zespołu CERT Polska, zajmującego się profesjonalnie problematyką bezpieczeństwa teleinformatycznego. Autorzy raportu z badań formułują m.in. następujące wnioski:

- Aplikacje filtrujące nie są w stanie monitorować całej zawartości Internetu. Ich konstrukcja opiera się na rozwiązaniach statycznych, podczas gdy Internet jest medium podlegającym nieustannym zmianom. Skutecznie można jedynie filtrować pewien wycinek globalnej Sieci. Podstawowym ograniczeniem jest wielojęzyczność serwisów internetowych – jakość filtrowania zależy między innymi od zbioru stałych kryteriów (słów kluczowych), których liczba jest praktycznie nieograniczona.[22]

[20] Na podstawie raportu NASK „Jak skutecznie filtrować zawartość Internetu" opracowanego w 2007 roku w ramach programu Safer Internet w Polsce.
[21] Niektóre z komercyjnych programów udostępniają bezpłatnie: okrojone i/lub ograniczone czasowo bezpłatne wersje testowe. Jednym z nielicznych w pełni bezpłatnych, popularnych filtrów jest program „Beniamin".
[22] Na podstawie raportu NASK „Jak skutecznie filtrować zawartość Internetu"

- Filtry nie są w stanie dokonać inteligentnego rozpoznania kontekstu i grafiki. Nielegalne lub szkodliwe treści mogą zostać mylnie otagowane, umieszczone w neutralnym kontekście, bądź opisane za pomocą neutralnych słów-kluczy. Jednocześnie aplikacja filtrująca może blokować portale edukacyjne czy encyklopedie ze względu na to, że hasła odnoszące się do rozwoju płciowego człowieka będą przez nią identyfikowane jako treści zabronione.

- Programy filtrujące w niedostateczny sposób rozpoznają takie zawartość Web 2.0 – serwisów społecznościowych, blogów, fotoblogów oraz portali zawierających pliki muzyczne i filmowe.

- Większość aplikacji nie zawiera wykazu blokowanych kategorii, co może utrudnić administratorom (rodzicom, opiekunom, nauczycielom) właściwą i pożądaną ze względu na dobro rozwoju dziecka konfigurację programu.

Pomimo ograniczeń oprogramowania filtrującego może ono wesprzeć dorosłych w zapewnianiu dzieciom bezpieczeństwa *on-line.* Ważne jest jednak, żeby mieli oni świadomość tych ograniczeń i stosowali tego typu oprogramowanie przy równoczesnym z podejmowaniu szeregu działań edukacyjnych i wspierających dziecko w korzystaniu z Sieci. Ważne jest też, żeby dorośli, decydujący się na stosowanie filtrów, wykorzystywali w pełni ich możliwości polegające m.in. na ustawianiu odpowiedniego do wieku poziomu filtrowania, ustawianiu indywidualnych profili dla każdego dziecka, przeglądaniu i weryfikowaniu tzw. białych i czarnych list (czyli stron bezwarunkowo blokowanych lub udostępnianych), czy regularnym aktualizowaniu programu (*update*). Programy tego typu znajdują szczególne zastosowanie w szkołach, gdzie ze względu na ograniczone możliwości osobistej kontroli stanowisk komputerowych przez nauczycieli mogą stanowić ważny element kontroli.

„Drugim poziomem są serwery usługowe utrzymywane przez providerów, którzy mogą prowadzić stały monitoring treści zamieszczonych w przestrzeni klienta. Zabezpieczenia tego rodzaju wymagają inwestycji finansowych oraz świadomości właścicieli serwisów o zagrożeniach jak i o skuteczności działania określonych zabezpieczeń.

Trzeci poziom – to filtrowanie treści na poziomie sieci dostępowej realizowane przez dostawców Internetu. Jest to jeden z najskuteczniejszych sposobów. Przedsięwzięcie to wymaga jednak akceptacji i koordynacji wszystkich dostawców działających na terenie kraju. Realizacja takiego filtrowania oprócz dużych nakładów finansowych wymaga także uregulowań prawnych, które będą zalecać a najlepiej wymuszać od wszystkich

dostawców takiego działania. Nie zawsze filtrowanie treści w Internecie jest akceptowane społecznie, jednak w przypadku pornografii dziecięcej, działanie takie nie powinno wywoływać protestów (…) Filtrowanie na poziomie sieci od miesiąca działa we Francji, na podstawie podpisanego porozumienia pomiędzy rządem francuskim a France Telecom. W ubiegłym roku filtrowanie na poziomie sieci włączone zostało w państwach skandynawskich. Bez decyzji rządu i odpowiednich uregulowań prawnych nie będzie możliwości filtrowania na ogólnym poziomie. Podobnie skuteczność działania zarówno zespołów reagujących jak i policji oraz administratorów wymaga wielu uregulowań prawnych" – mówi kierownik Dyżurnetu, Marek Dudek.

Pomoc w dbaniu o bezpieczeństwo dzieci *on-line* mają też zapewniać rozwiania z kategorii „Kontrola rodzicielska" (*parental control*) udostępniane jako oddzielne programy lub będące elementem systemów operacyjnych lub aplikacji internetowych. Dają one za zwyczaj szerokie spektrum możliwości kontrolowania poczynań dzieci w Internecie. Jednym z przykładów takiego rozwiązania są funkcje kontroli rodzicielskiej zastosowane w systemie Microsoft Vista dające m.in. możliwość:

- Ograniczenia dostępu dzieci do wybranych treści w Sieci
- Ustalenia limitu czasu korzystania z komputera i Internetu
- Kontroli dostępności wybranych programów i aplikacji
- Kontroli dostępności do wybranych gier

Programy tego typu dają też czasami możliwość śledzenia aktywności dzieci online, włącznie z raportowaniem rodzicom treści rozmów i korespondencji prowadzonych przez dziecko przy użyciu Internetu.

Podobnie jak w przypadku oprogramowania filtrującego, programy służące kompleksowej kontroli rodzicielskiej mogą stanowić ważny element działań, mających na celu zapewnienie dziecku bezpieczeństwa w Internecie, ale nie są to narzędzia doskonałe. Dodatkowo wymagają one od rodziców pewnego poziomu wiedzy i umiejętności związanych z korzystaniem z komputera i Internetu. Istotnie kontrowersyjne wydają się programy pozwalające na inwigilowanie dzieci *on-line*. Wydaje się, że minimalnym warunkiem stosowania przez rodziców takich aplikacji jest wcześniejsze poinformowanie o tym dziecka

3.5 Profilaktyka zagrożeń podejmowana przez dostawców usług

Dzieci powszechnie korzystają w Internecie z serwisów społecznościowych, kontaktują się między sobą, zawierają nowe znajomości, poznają i pozyskują nowe treści..[23] Popularność sieci Web 2.0 wskazywana jest przez specjalistów jako jedno z większych zagrożeń dla bezpieczeństwa najmłodszych internautów. Na tym polu oprogramowanie filtrujące znajduje mocno ograniczone zastosowanie a i edukacja, nawet intensywna nie jest w stanie uchronić dzieci przed wszystkimi zagrożeniami. W takiej sytuacji niezmiernie ważne jest zaangażowanie się dostawców usług w przeciwdziałanie problemowi, które polegać powinno przede wszystkim na:

- kontrolowaniu treści udostępnianych dzieciom
- moderowaniu kontaktów *on-line*
- udostępnianiu treści edukacyjnych związanych z bezpieczeństwem *on-line*
- zapewnianiu szybkiej interwencji w sytuacji zagrożenia

Przedstawiciele branży internetowej coraz częściej podejmują indywidualne lub branżowe działania w zakresie bezpieczeństwa dzieci. Aktywności takie są też inspirowane bądź narzucane przez instytucje rządowe oraz międzynarodowe, wspierane przez odpowiednie zapisy prawne. W USA np. lobbing na rzecz zapewnienia dzieciom bezpieczeństwa *on-line* skłonił dwa największe portale społecznościowe Facebook i Myspace do przyjęcia programu walki z zagrożeniami dzieci. Przyjęte przez nie zobowiązania polegają m.in. na:

- zobowiązaniu nowych użytkowników do zapoznania się ze strefą „safety tips", czyli informacjami i poradami związanymi z bezpiecznym korzystaniem z serwisu;
- zapewnieniu dzieciom możliwości łatwego i szybkiego informowania odpowiednich służb o zagrożeniach lub popełnianych czynach zabronionych ('report abuse");
- uniemożliwieniu dorosłym użytkownikom zmiany tożsamości, polegającej na obniżaniu w profilu użytkownika deklarowanego wcześniej wieku.
- opracowywaniu behawioralnego systemu rozpoznawania wieku, polegającego m.in. na analizie kontaktów interpersonalnych realizowanych w serwisie.
- usuwanie materiałów zgłaszanych jako niewłaściwe w czasie nie dłuższym 24 godziny.

[23] W Stanach Zjednoczonych do najpopularniejszych wśród dzieci i młodzieży serwisów społecznościowych należą MySpace i Facebook. Najpopularniejsze w Europie są Bebo, MySpace, Skyrock Blog, oraz Facebook (źródło: wikipedia). W Polsce dużą popularnością cieszą się EPuls.pl oraz Grono.net

Nad opracowaniem podobnych regulacji pracuje także Komisja Europejska planująca ujednolicenie regulaminów i polityki prywatności serwisów społecznościowych.[24]

3.6 Wsparcie organów ścigania w zwalczaniu przestępczości wobec dzieci

Rozwiązania technologiczne , obok odpowiednich regulacji prawnych, są podstawą zwalczania przestępczości wobec dzieci w Internecie. Znajdują one już od lat zastosowanie w zwalczaniu przestępstw związanych z rozprowadzaniem i publikowaniem w Sieci pornografii dziecięcej. Specjalistyczne bazy danych dają możliwość policji oraz międzynarodowym strukturom, zwalczającym przestępczość *on-line*, jak Interpol, możliwość sprawdzania, czy zabezpieczone w toku działań operacyjnych materiały pornograficzne z udziałem dzieci były już wcześniej przedmiotem zainteresowania organów ścigania i czy udało się w toku wcześniej podejmowanych działań dotrzeć do ofiar oraz sprawców tych przestępstw. Urządzenia takie są niezwykle zaawansowane technologicznie i coraz skuteczniejsze dzięki olbrzymim nakładom finansowym i zaangażowaniu w ich tworzenie międzynarodowych gremiów naukowców[25]. Ze względu na masowy i transgraniczny charakter problemu pornografii dziecięcej bazy danych są niezbędnym narzędziem pracy dla policji na całym świecie.

Nowoczesna technologia znajduje również zastosowanie w walce z procederem uwodzenia dzieci w Sieci. Naukowcy pracują intensywnie nad wykorzystywaniem w tym celu sztucznej inteligencji. Precyzyjnie opracowane programy przeszukiwać i analizować mają rozmowy oraz inne aktywności w Sieci, szczególnie w serwisach popularnych wśród dzieci, szukając sekwencji zdarzeń właściwych dla procesu uwodzenia małoletnich.[26]

[24] Do prac nad projektem kodeks postępowania dla serwisów społecznościowych Komisja Europejska zaprosiła wiodące światowe portale, jak Facebook, MySpace, YouTube oraz Yahoo. Spośród pośród polskich serwisów społecznościowych do współpracy zaproszono Epuls i Grono.net.

[25] Np. baza *Intertional Child Sexual Exploitation Image Database* wykorzystywna m.in. przez Interpol zawiera ponad 500 000 zidentyfikowanych materiałów pornograficznych z udziałem dzieci oraz 20 000 zidentyfikowanych ofiar.

[26] Grupa polskich naukowców wspierana przez Ministerstwo Nauki i Szkolnictwa Wyższego oraz Wyższą Szkołę Handlu i Finansów Międzynarodowych w Warszawie opracowuje program Cerber, wyposażony w sztuczną inteligencję i analizator języka naturalnego, który już od jesieni 2008 roku ma być wykorzystywany prze Policje w celu analizowania czatów popularnych wśród dzieci w Polsce.

Postulowane kierunki zmian:

Profesjonaliści z branży technologicznej zwracają uwagę na następujące kwestie związane z wykorzystywaniem technologii w walce z zagrożeniami wobec dzieci w Internecie:[27]

1. Konieczność koordynacji i synchronizacji różnych pomysłów z zakresu prawa i edukacji z możliwościami technologicznymi i doświadczeniami z działanie już wprowadzonych technicznych mechanizmów bezpieczeństwa
2. Uwzględnienie zasad ochrony prywatności w działaniach technicznych w sieci tak, aby nowe rozwiązania nie naruszały prawa do prywatności osób, które nie mają nic wspólnego z naruszeniem bezpieczeństwa w Internecie
3. Uwzględnianie rodzajów zagrożeń technicznych w programach edukacyjnych przygotowywanych dla poszczególnych grup odbiorców (np.: rodziców, nauczycieli, zwykłych użytkowników Internetu)
4. Wprowadzanie technik bezpieczeństwa przez producentów czy operatorów telekomunikacyjnych na zasadach samoregulacji opartych o najlepsze praktyki z danej dziedziny, jednocześnie warto się zastanowić nad wprowadzeniem minimalnych obowiązków związanych z ochroną sieci, np.: konieczności zgłaszania przypadków naruszania bezpieczeństwa teleinformatycznego dotyczących tzw. Infrastruktury krytycznej
5. Zdecydowana większość problemów w sieci to problemy wykraczające poza obszar jednego państwa, dlatego wszelkie rozwiązania techniczne powinny uwzględniać uwarunkowania i współpracę międzynarodową
6. Należy tak wzmocnić wszelkiego rodzaju służby działające na rzecz bezpieczeństwa Internetu, tak aby nie pozostawały one w dziedzinie technologii i wiedzy z przestępcami sieciowymi

[27]Wnioski z panelu dyskusyjnego z udziałem profesjonalistów z zakresu nowych technologii zorganizowanego w ramach seminarium „Bezpieczeństwo dzieci w Internecie" (organizacja: FDN, Microsoft, Warszawa 10 kwietnia 2008). Postulaty przytoczone za wydawnictwem pokonferencyjnym.

IV Bezpieczeństwo dzieci i młodzieży w Internecie – współpraca międzynarodowa

Ze względu na globalny charakter internetowych zagrożeń, współpraca międzynarodowa oraz działania podejmowane na najwyższym szczeblu różnych organizacji międzynarodowych odgrywają ogromną rolę w przeciwdziałaniu przestępstwom komputerowym wobec dzieci i młodzieży. Efektem takich działań są międzynarodowe projekty legislacyjne, transgraniczna współpraca organów ścigania, międzynarodowe projekty edukacyjne oraz wymiana dobrych praktyk, pozwalająca na doskonalenie działań narodowych.

4.1 Działania w obrębie Unii Europejskiej

Tematyką bezpieczeństwa w Internecie od 1996 roku zajmuje się Unia Europejska. W 1996 roku opierając się na artykule K.3 Traktatu w Maastrich, Rada Unii Europejskiej przyjęła plan walki z rasizmem i ksenofobią"[28]. W 1997 roku Rada ds. Telekomunikacji przyjęła rezolucję w sprawie szkodliwych lub nielegalnych treści w Internecie[29], Komisja Europejska zaś wydała oświadczenie pod tytułem „Nielegalne i szkodliwe treści w Internecie", w którym podkreślono „wysoce zdecentralizowaną i transnarodową naturę Internetu" i rekomendowano „skoordynowaną reakcję na międzynarodowym i europejskim szczeblu". Wkrótce potem Parlament oraz Rada Europejska opracowały „Plan działania w zakresie promocji bezpiecznego korzystania z Internetu poprzez walkę ze szkodliwymi lub nielegalnymi treściami w globalnych sieciach", który stał się impulsem do uruchomienia przez Komisję Europejską kompleksowego programu pod nazwą *Safer Internet Action Plan* (SIAP). Program został pierwotnie przyjęty na lata 1999-2002 roku. W okresie tym dofinansowanych zostało 37 projektów. Kolejna edycja programu realizowana w latach 2003-04 pozwoliła na dofinansowanie aż 52 projektów.

Obecnie realizowana edycja programu, pod nazwą Safer Internet plus, jest kontynuacją programu Safer Internet Action Plan z lat 1999-2004. Zakres programu Safer Internet plus został poszerzony i obejmuje obecnie także telefonię komórkową, przekaz szerokopasmowy, gry online, wymiany plików przez sieci peer-to-peer i wszystkie formy komunikacji w czasie rzeczywistym, takie jak czaty i komunikatory internetowe. [30]

[28] OJ L 185/5 z 25.7.1996
[29] OJ C 70/1 z 6.3.1997
[30] W Polsce konsorcjum FDN i NASK realizuje od 2005 rokuw ramach programu Safer Internet projekty projekt Awareness, Hotline i Helpline

Program Safer Internet plus obejmuje 4 główne działania; są to:

- **Promocja bezpiecznego korzystania z Internetu**
- **Walka z nielegalnymi treściami**
- **Zwalczanie niepożądanych i szkodliwych treści**
- **Promocja bezpiecznego środowiska**

Integralną częścią każdej z powyższych akcji jest szeroko rozwinięta współpraca międzynarodowa[31].

Promocja bezpiecznego i efektywnego korzystania z Internetu jest jednym z podstawowych założeń programu Safer Internet. Od 2004 roku w całej Europie powstają narodowe punkty (tzw. *Awareness Nodes*), które odpowiedzialne są za kompleksowe działania edukacyjne na rzecz bezpiecznego i efektywnego korzystania z Sieci. Koordynatorzy projektu *Awareness* w poszczególnych krajach wyłaniani są w drodze otwartego konkursu wniosków ogłaszanego przez Komisję Europejską. Na poziomie krajowym punkty te zapewniają wymianę dobrych praktyk oraz kształcenie dzieci, rodziców i nauczycieli.

Realizatorzy projektu z całej Europy zrzeszeni są w sieci INSAFE, której koordynatorem jest organizacja European Schoolnet z Brukseli. Do INSAFE należą obecnie organizacje z 27 krajów europejskich (www.saferinternet.org). Dodatkowo INSAFE współpracuje z organizacjami z krajów stowarzyszonych, takich jak Australia, Stany Zjednoczone, Rosja, Argentyna, Kanada, Singapur.
INSAFE pełni funkcję eksperta i obserwatora przy Komisji Rady Europy ds. Mediów i Społeczeństwa Informacyjnego (Media and Information Society Division). Wniósł także istotny wkład w powstanie opublikowanego przez Radę Europy wielojęzycznego podręcznika zatytułowanego Internet Literacy Handbook. Podręcznik ukazał się w 8 językach i został rozdystrybuowany w setkach tysięcy egzemplarzy na całym świecie. Na jego podstawie opracowano nową grę internetową poświęconą bezpieczeństwu w Sieci, „Przez dzikie internetowe lasy" (Through the Wild Web Woods). Gra posiada również polską wersję językową.

[31] Więcej informacji: http://ec.europa.eu/information_society/activities/sip

INSAFE jest przykładem międzysektorowego podejścia do bezpieczeństwa w Internecie. Organizacje członkowskie wywodzą się ze wszystkich sektorów społecznych: od organizacji ze sfery pozarządowej, organizacji rządowych, po firmy komercyjne. Podobne zróżnicowanie występuje jeśli chodzi o profil organizacji – w poszczególnych krajach europejskich w działania edukacyjne w ramach programu Safer Internet zaangażowane są organizacje pozarządowe zajmujące się prawami dzieci (Polska, Hiszpania, Finlandia, Włochy), ministerstwa edukacji (Francja, Portugalia), instytuty ds. telekomunikacji (Austria), rady ds. mediów (kraje skandynawskie: Szwecja, Norwegia), uniwersytety (Słowenia), organizacje konsumenckie (Belgia), firmy informatyczne (Luksemburg). W wielu krajach tworzone są konsorcja, składające się z 2-3 organizacji o uzupełniającym się profilu, które pozwalają na prowadzenie bardziej kompleksowych działań edukacyjnych oraz zapewnienie ich lepszego zasięgu.

Działania wszystkich narodowych koordynatorów programu Safer Internet podejmowane są w ścisłej współpracy z różnymi interesariuszami na poziomie krajowym - w ramach projektu tworzone są ciała doradcze (tzw. Advisory Board) przy programie Safer Internet, w skład których wchodzą przedstawiciele głównych ministerstw, policji, organizacji działających na rzecz dzieci, uczelni wyższych zajmujących się tematyką Internetu i nowych mediów. Do zadań takich podmiotów

należy pomoc w planowaniu i optymalizacji działań na rzecz bezpieczeństwa w Internecie, wzajemna wymiana informacji i dobrych praktyk, a także ocena już przeprowadzonych przedsięwzięć.

Warto również wspomnieć, że od 2007 roku w ramach programu Safer Internet plus dofinansowywane są Helpline'y - czyli linie pomocowe, gdzie dzieci, młodzież, rodzice i profesjonaliści pracujący z dziećmi mogą zgłaszać przypadki zagrożen w Internecie, takich jak np. uwodzenie dzieci (grooming), cyberprzemoc, kontakt ze szkodliwymi treściami, uzależnienia od Internetu. Helpline'y są bardzo istotnym uzupełnieniem akcji edukacyjnych, a mając codzienny kontakt z młodymi internautami pomagają w planowaniu działań profilaktycznych, wskazując na obszary największych zaniedbań jeśli chodzi o zagrożenia w Internecie.

W ramach programu Safer Internet Komisja Europejska od 1999 roku aktywnie wspiera **walkę z nielegalnymi treściami w Internecie**. W większości krajów europejskich działają Hotline'y, których misją jest przyjmowanie zgłoszeń o nielegalnych treściach znalezionych przypadkowo w Sieci, takich jak pornografia dziecięca, rasizm, ksenofobia. Duża wrażliwość użytkowników Sieci sprawia, że do hotline'ów często zgłaszane są treści takie jak namawianie do popełnienia samobójstwa, zażywania narkotyków, etc. – które w większości krajów nie podlegają penalizacji.

Hotline zrzeszone są w Stowarzyszeniu INHOPE (The Association of Internet Hotline Providers), w ramach którego mają możliwość bliskiej współpracy z hotline'ami z innych krajów oraz wspólnego wypracowywania standardów i procedur. Aktualnie INHOPE skupia 33 zespoły z krajów europejskich i z innych części świata, w tym z Ameryki Północnej, Australii i Azji.

Hotline'y w poszczególnych krajach działają w bliskiej współpracy z policją, organizacjami rządowymi i pozarządowymi, z dostawcami usług i treści internetowych (ISP i ICP). Wszystkie zgłoszenia otrzymane przez hotline poddawane są dokładnej analizie. W przypadku treści nielegalnych z puntku widzenia prawa w danym kraju, hotline przekazuje zgłoszenie do właściwych podmiotów, którymi mogą być policja, dostawca usług internetowych (tzw. ISP), hotline w innym kraju, w zależności od lokalizacji serwera i zgodnie z wewnętrznymi procedurami postępowania. Czasami zdarza się, że serwer z nielegalnymi treściami umiejscowiony jest w państwie, gdzie nie działa narodowy hotline - wtedy zgłoszenie zostaje przekazane policji w danym kraju. Pozytywne zakończenie wielu spraw bywa utrudnione ze względu na różnorodność prawa w poszczególnych państwach (vide tzw. wirtualna pornografia dziecięca, strony promujące anoreksję i bulimię).

Program Safer Internet plus promuje także tworzenie efektywnych narzędzi technicznych, takich jak programy filtrujące, które mogą pomóc rodzicom w zwalczaniu niepożądanych i szkodliwych treści, na które narażone są dzieci (np. zawierające pornografię reklamy).

Od 2006 roku realizowany jest program badawczy pod nazwą SIP-BENCH (http://www.sip-bench.eu). Jego koordynatorzy - firma Deloitte oraz uniwersytet w Leuven - prowadzili badania oprogramowania filtrującego dostępnego na rynkach europejskich, które mają dostarczyć eksperckiej, niezależnej od producentów i sprzedawców oceny kilkudziesięciu technicznych rozwiązań. Wyniki badań posłużą do propagowania najlepszych praktyk, dostarczenia odpowiednich wskazówek rodzicom, edukatorom, oraz producentom i sprzedawcom.

Komisja Europejska kładzie także duży nacisk na **promocję tematyki bezpieczeństwa w Internecie** wśród różnych sektorów społecznych. Temu ma służyć m.in. powołanie corocznych spotkań pod nazwą Safer Internet Forum, które umożliwiają przedstawicielom biznesu, polityki i organizacji działających na rzecz dzieci dyskusję o bezpieczeństwie w Internecie oraz pomagają wypracować nowe sposoby promocji przyjaznego najmłodszym środowiska wirtualnego. Ponadto, regularnie ogłaszane są otwarte konsultacje publiczne, na wybrane tematy związane z ochroną dzieci i młodzieży w świecie wirtualnym. Komisja jest także aktywnym inicjatorem szeregu działań z zakresu samoregulacji. Z inicjatywy Komisji Europejskiej w 2007 roku wypracowane zostało „Porozumienie na rzecz bezpiecznego korzystania z telefonów komórkowych przez dzieci i młodzież", które zostało podpisane w Brukseli w Dniu Bezpiecznego Internetu w 2007 roku, przez wiodących operatorów telefonii komórkowej. Osiągnięte porozumienie było odpowiedzią na liczne obawy wyrażone w trakcie zorganizowanych wcześniej przez Komisję publicznych konsultacji, dotyczących bezpiecznego korzystania z telefonów komórkowych, wskazujące na szereg zagrożeń związanych z telefonią mobilną oraz niską świadomością rodziców. Porozumienie podpisały następujące firmy: Orange Group, Bouygues Telecom, Cosmote, Debitel AG, Deutsche Telekom Group, Go Mobile, Hutchison 3G Europe, Jamba! GmbH, Mobile Entertainment Forum, Royal KPN N.V., SFR, Telecom Italia S.p.ATelefonica Moviles S.A., Telenor, TeliaSonera oraz Vodafone Limited.

Porozumienie przewiduje wypracowanie kodeksów samoregulacji i podjęcie działań na rzecz ochrony dzieci, takich jak:

- wspieranie kontroli dostępu do treści przeznaczonych dla dorosłych,
- prowadzenie kampanii informacyjnych skierowanych do rodziców i dzieci,
- klasyfikację treści komercyjnych według krajowych standardów dobrych obyczajów,
- zwalczanie naruszających prawo treści w sieciach komórkowych.

Komisja Europejska jako inicjator porozumienia obserwuje postęp prac sygnatariuszy.
Obecnie podobny Kodeks Postępowania wypracowywany jest przez przedstawicieli serwisów społecznościowych. Ma on ujednolicić regulaminy i politykę prywatności popularnych wśród dzieci i

młodzieży serwisów społecznościowych. Kodeks ma poruszać zagadnienia takie jak ochrona prywatności, filtrowanie treści oraz kwestie moderacji i raportowania o nadużyciach.

Twórcy serwisów społecznościowych wykazują gotowość do podjęcia współpracy w tej kwestii, ponieważ im również zależy na bezpieczeństwie swoich użytkowników. Twórcy Bebo.com, jednej z największych społecznych sieci medialnych na świecie, dającej m.in. możliwość przeglądania, tworzenia, wyszukiwania i dzielenia się treściami generowanymi przez profesjonalistów oraz samych użytkowników, zrzeszającej 11,4 mln unikalnych użytkowników w Wielkiej Brytanii i łącznie ponad 40 milionów zarejestrowanych użytkowników na całym świecie tak oto komentują zagadnienie bezpieczeństwa Sieci:

„Miliony ludzi korzystają obecnie z internetowych serwisów społecznościowych umożliwiających wirtualną komunikację i poznawanie nowych ludzi oraz prezentowanie swoich zdolności w sieci. Serwisy społecznościowe działają w oparciu o technologię web 2.0, co w skrócie oznacza, że rozwijają się dynamicznie dzięki treściom dodawanym przez użytkowników, którzy w ten sposób nadają stronom ostateczny kształt.

Internet zmienia styl naszego życia i nigdzie nie widać tego tak wyraźnie, jak w środowisku współczesnych i następnych pokoleń nastolatków. Dzieci dorastają w ścisłej styczności z technologią komputerową – zdecydowana większość treści zamieszczanych w serwisie Bebo pochodzi od komunikujących się między sobą nastolatków.

Dorosłym, w tym nauczycielom, którzy nie znają wspomnianej technologii i mają poczucie, że to zupełnie inny świat, nad którym nie sprawują żadnej kontroli, taka perspektywa może wydać się zniechęcająca. Jednak wcale tak być nie musi i osoby, które generalnie swobodnie radzą sobie z obsługą komputera, nie muszą uważać serwisów pokroju Bebo za obszary nieprzeniknione.

W rzeczywistości zrozumienie działania podobnych serwisów przez osoby dorosłe ma zasadnicze znaczenie z punktu widzenia informowania i edukacji młodzieży, jak korzystać z tego rodzaju stron w sposób bezpieczny i właściwy. Chociaż serwisy te służą przede wszystkim komunikowaniu się ze znajomymi i poznawaniu nowych ludzi, niektórzy mogą je wykorzystywać w bardziej negatywnych celach do nękania, wyszydzania i zastraszania innych, a w bardziej ekstremalnych przypadkach pedofile mogą próbować za ich pośrednictwem nawiązać znajomość z młodymi ludźmi.

W związku z powyższym nieodzowna jest praca z uczniami, aby przekazać im umiejętności możliwie najlepszego wykorzystania serwisów społecznościowych, a jednocześnie nauczyć ich, jak chronić się przed osobami, które mogą być dla nich niebezpieczne.

Dlatego właśnie w maju 2008r serwis internetowy Bebo ogłosił uruchomienie serwisu edukacyjnego przygotowanego z myślą o zachęceniu nauczycieli i młodzieży do wspólnej dyskusji na temat bezpiecznego i odpowiedzialnego korzystania z Internetu, w szczególności internetowych serwisów społecznościowych. Serwis edukacyjny dostarcza nauczycielom materiały, które mogą być przez nich używane na zajęciach lekcyjnych do

przekazywania wiedzy i pomocy młodym ludziom w zrozumieniu kwestii związanych z osobistym bezpieczeństwem w sieci internetowej.

Bebo to pierwszy serwis społecznościowy, który stworzył tego typu internetowy serwis edukacyjny dla szkół, dostępny pod adresem URL www.safesocialnetworking.com. W wyniku współpracy Bebo ze specjalistami w dziedzinie programów nauczania powstały materiały dydaktyczne dostosowane do celów nauczania i wpisujące się w istniejące rozkłady zajęć. Serwis został przygotowany w taki sposób, aby dyskusje na temat bezpieczeństwa w sieci za pomocą odnośnych materiałów mógł przeprowadzić każdy nauczyciel, bez względu na stopień przygotowania informatycznego.

*Z przeprowadzonego ostatnio badania*32 wynika, że 90% nauczycieli informatyki i dyrektorów szkół uważa, że ich uczniowie wiedzą o technologii komputerowej więcej niż oni. Wielu nauczycieli nie posiada podstawowej wiedzy na temat serwisów społecznościowych, co otwiera przepaść pokoleniową pomiędzy nimi a ich młodymi podopiecznymi, którzy coraz chętniej komunikują się przez Internet.*

- Zamiarem Bebo jest zapewnienie wsparcia dyrektorom szkół i nauczycielom poszukującym dialogu na temat bezpiecznego i odpowiedzialnego korzystania z Internetu zarówno w szkole, jak i poza nią. Mamy nadzieję, że przygotowany serwis edukacyjny pomoże nauczycielom znaleźć wspólny język z uczniami, który pozwoli im autorytatywnie wypowiadać się na temat bezpieczeństwa w sieci internetowej. - mówi Dr Rachel O'Connell, Dyrektor ds. Bezpieczeństwa Bebo.

Przygotowane materiały dydaktyczne obejmują arkusze robocze, uwagi dla nauczyciela, słowniczek internetowy oraz zestaw krótkich filmów wideo i animacji przekazujących wiadomości na temat bezpieczeństwa on-line w sposób wyczerpujący, a zarazem zajmujący. Materiały są dostępne na stronie serwisu Bebo poświęconej kwestiom bezpieczeństwa (www.bebo.com/safety), jednak podjęta przez wiele szkół decyzja o zablokowaniu dostępu do serwisów społecznościowych w szkolnych pracowniach komputerowych oznacza, że dotychczas nauczyciele nie mieli możliwości w pełni wykorzystać tych zasobów. Uruchomienie niezależnego serwisu wyeliminuje tę przeszkodę.

- Obecnie istnieje przepaść pomiędzy tym, co o serwisach społecznościowych wiedzą nauczyciele, a tym, jak korzystają z nich uczniowie w klasach. Musimy tę przepaść pokoleniową zasypać i przygotowane zasoby dydaktyczne stanowią ważny krok, aby ten cel osiągnąć. - mówi Ruth Hammond, Kierownik ds. Programów Ochrony Bezpieczeństwa brytyjskiej agencji rządowej Becta.

- Bebo opracowuje materiały dydaktyczne we współpracy z englishdatabase.com. Englishdatabase.com posiada akredytację rządowego serwisu internetowego na rzecz technologii informacyjnych w oświacie Curriculum On-line."

32 Badanie przeprowadzone przez operatora rozwiązań szerokopasmowego dostępu do Internetu ZyTEL Communications na targach technologii informacyjnych w edukacji BETT 2008

4.2 Działania ONZ

Oprócz działań Komisji Europejskiej tematyka bezpieczeństwa dzieci i młodzieży w Internecie znalazła ostatnio swoje miejsce także w łonie Organizacji Narodów Zjednoczonych. W ramach zwołanego przez Sekretarza Generalnego ONZ w listopadzie 2007 roku w Rio de Janeiro Forum Zarządzania Internetem (**Internet Governance Forum**) problematyka ochrony dzieci *on-line* była wielokrotnie wyraźnie akcentowana, na czele z entuzjastycznie przyjętymi przez organizacje działające na rzecz dzieci słowami Sekretarza Generalnego ONZ, Ban Ki-Moona, który w swym przemówieniu inauguracyjnym podkreślił konieczność zwiększenia wysiłków na rzecz bezpieczeństwa dzieci w Internecie. W Forum uczestniczyło ponad 1300 ekspertów z całego świata, wśród nich wysocy przedstawiciele instytucji rządowych, sektora pozarządowego, dostawców usług i treści internetowych oraz instytucji regulacyjnych. IGF jest ciałem doradczym, bez stałego członkostwa i bez mocy decyzyjnej; spotkania Forum są otwarte i mają charakter dialogu politycznego.

Konkretnym zyskiem ze spotkania było stworzenie tzw. **„Dynamicznej Koalicji na rzecz Bezpieczeństwa Dzieci w Internecie"** *(Dynamic Coalition on Child Online Safety)*.[33] Ideą przyświecającą powołaniu tej grupy było dążenie do połączenia maksymalnej otwartości i dostępność w sieci z zapewnieniem tam bezpieczeństwa, głównie najmłodszym. Dynamiczne koalicje mają charakter międzysektorowy i mogą być zakładane przez same zainteresowanymi podmioty uczestniczące w IGF. „Dynamiczna Koalicja na rzecz Bezpieczeństwa Dzieci w Internecie" skupia głównie przedstawicieli organizacji, pracujących na rzecz ochrony dzieci oraz zwolenników wolności słowa w Sieci. Koalicja ta pozostaje otwarta na współpracę również z innymi zainteresowanymi podmiotami. Oprócz międzysektorowej dyskusji, wymiany doświadczeń i dobrych praktyk, jednym z celów Koalicji jest przedstawienie propozycji sesji poświęconej bezpieczeństwu dzieci *on-line*, która zostałaby wpisana w program przyszłorocznego Forum w Indiach w grudniu 2008 roku.

[33] Polskę w koalicji reprezentuje Fundacja Dzieci Niczyje

4.3 Przykłady dobrych praktyk międzynarodowych

Inicjatywy łączące szereg krajów we wspólnej akcji, takie jak Dzień Bezpiecznego Internetu (*Safer Internet Day*), można uznać za najlepsze praktyki w działaniach na rzecz bezpieczeństwa dzieci, niosące dużą wartość dodaną i pozwalające dzięki udziałowi mediów na dotarcie do szerokich grup odbiorców.

Dzień Bezpiecznego Internetu obchodzony jest od 2005 roku w lutym, z inicjatywy Komisji Europejskiej. Inicjatywa ta ma na celu zwrócenie uwagi na kwestię bezpiecznego korzystania przez dzieci i młodzież z zasobów internetowych. Patronat nad obchodami DBI obejmuje co roku Komisarz Unii Europejskiej ds. Społeczeństwa Informacyjnego i Mediów.

W poszczególnych krajach za organizację Dnia Bezpiecznego Internetu odpowiadają organizacje uczestniczące w projekcie Safer Internet. Oprócz krajów europejskich inicjatywa ta zyskała uznanie także poza naszym kontynentem – w obchody DBI dorocznie włącza się także Kanada, Stany Zjednoczone, Singapur, Rosja, Japonia, Argentyna, kraje Ameryki Środkowej – łącznie co roku organizacje z około 60 państw.

Dorocznie obchodom Dnia Bezpiecznego Internetu w całej Europie towarzyszą festyny, projekty, dyskusje oraz wystawy, promujące odpowiedzialne postawy dorosłych oraz prawo dzieci do bezpiecznego korzystania z Internetu. W ramach sieci INSAFE co roku organizowany jest międzynarodowy konkurs dla szkół dotyczący tematyki internetowej. Zwycięzcy z reguły ogłaszani są w Dniu Bezpiecznego Internetu przez Komisarz UE ds. Społeczeństwa Informacyjnego i Mediów. Nagrodami dla zwycięskich szkół były dotychczas atrakcyjne dotacje na zakupy związane z technologiami ICT.

Sieć INSAFE od lat współpracuje w swoich działaniach z **firmami komercyjnymi**, które z racji bezpośredniego zaangażowania w rozwój nowych technologii, stają się szczególnie cennym partnerem. Europejskimi partnerami Dnia Bezpiecznego Internetu były dotychczas firmy UPC oraz Vodafone.

W 2008 roku z okazji DBI firma UPC we współpracy z INSAFE przygotowała **podręcznik pod tytułem "Bezpieczeństwo w sieci - elementarz dla całej rodziny"**. Publikacja ta jest przeznaczona dla rodziców oraz dzieci w wieku od 6 do 12 lat. Ma im pomóc we wspólnym przygotowaniu się do korzystania z komputera i Internetu, we wspólnym „oswajaniu sieci". Pokazuje m.in. jak Internet może integrować rodzinę, zwracając jednak uwagę na główne zagrożenia.

Kolorowa teczka mieści w sobie dwie broszury, jedną przeznaczoną dla dzieci, drugą dla rodziców. Do wydawnictwa dołączono też naklejki, karty z opisami różnych sytuacji oraz dyplom dla

całej rodziny. Podręcznik zapewnia dzieciom naukę połączoną z zabawą, a rodzicom wiedzę, która pozwoli im zostać przewodnikiem po wirtualnym świecie dla dzieci i partnerem do dyskusji dla młodzieży. Obydwie części mają taką samą strukturę i analogiczne rozdziały, kolejne sekcje tematyczne pozwalają na przyswojenie tych samych informacji w sposób odpowiedni dla adresata dziecięcego lub dorosłego.

Elementarz porusza zagadnienia takie jak ochrona domowego komputera przed wirusami i złośliwymi programami, które łatwo przedostają się np. wraz ze ściąganymi z Internetu i popularnymi wśród dzieci grami. Radzi, jak walczyć ze spamem oraz jak bezpiecznie zakładać konta internetowe, aby nie były przechwytywane przez spamerów. Uczy bezpiecznego komunikowania się z innymi użytkownikami Sieci, pokazuje jak chronić swoje dane osobowe. Wyjaśnia także, czym jest cyberprzemoc, podaje jej przykłady i sposoby ochrony dzieci. Walory dydaktyczne podręcznika wzmacniają liczne ćwiczenia i testy, które dzieci mogą rozwiązywać razem z rodzicami. Rodzice i dzieci znajdą też w przewodniku przydatne adresy internetowe i telefoniczne, pod którymi można zasięgnąć porady lub sprawdzić posiadaną wiedzę.

Elementarz został opublikowany w 11 językach, w tym w języku polskim. Elektroniczna wersja podręcznika w formacie pdf można pobrać ze strony: www.upclive.pl/dzieci/2089/20897358.html.

Inną godną uwagi inicjatywą jest **platforma edukacyjna dla nauczycieli TeachToday:** www.teachdoay.eu, w której uruchomienie włączyły się takie firmy jak Orange, Telecom Italia, Google, Telefonica, Microsoft, Vodafone i MySpace. Portal wychodzi naprzeciw zróżnicowanym potrzebom nauczycieli, którzy powinni pomagać swoim uczniom w jak najpełniejszym wykorzystywaniu nowych technologii, a jednocześnie mieć świadomość pułapek, jakie czyhają na nieostrożnych użytkowników. Serwis ma służyć zwiększeniu wiedzy i kompetencji nauczycieli w zakresie ochrony dzieci i młodzieży *on-line* oraz wskazać sposoby postępowania w przypadku zagrożeń, z jakimi najmłodsi mogą zetknąć się podczas korzystania z Internetu oraz nowych technologii komunikacyjnych. Dotychczas strona uruchomiona została w 6 wersjach językowych: angielskiej, niemieckiej, hiszpańskiej, czeskiej, francuskiej i włoskiej. Polska wersja językowa ma ruszyć wkrótce.

Analizując działania organizacji koordynujących program Safer Internet w poszczególnych krajach europejskich, należy zauważyć, iż w ich wysiłkach profilaktycznych dominuje wypracowywanie i szeroka dystrybucja materiałów edukacyjnych w postaci ulotek, broszur, scenariuszy zajęć dla nauczycieli. Praktycznie wszyscy realizatorzy programu umożliwiają zainteresowanym pobieranie tych materiałów ze swoich stron internetowych. W zależności od

środków niektóre organizacje prowadzą kampanie medialne, które wspierają działania edukacyjne realizowane przez nich w innych wymiarach. Doskonałym przykładem wymiany dobrych praktyk na poziomie europejskim jest replikacja kampanii medialnych, możliwa dzięki przekazaniu przez organizację prowadzącą lub agencję – autora praw do kampanii organizacji partnerskiej w innym kraju.

Dużym sukcesem w tym względzie poszczycić się może niemiecki projekt **klicksafe.de**, realizowany przez konsorcjum dwóch instytucji publicznych: Urzędu ds. Mediów landu Nadrenii-Palatynatu (Landeszentrale für Medien und Kommunikation Rheinland-Pfalz, LMK) – koordynatora konsorcjum, oraz Urzędu ds. Mediów landu Północnej Nadrenii-Westfalii (Landesanstalt für Medien Nordrhein-Westfalen, LfM), przy wsparciu Europejskiego Centrum Kompetencji Medialnych (Europäisches Zentrum für Medienkompetenz, ecmc). Niemieckie Urzędy ds. Mediów odpowiadają za udzielanie zezwoleń na nadawanie oraz za nadzór nad komercyjnymi stacjami radiowymi i telewizyjnymi, a także za promowanie i rozwijanie edukacji w zakresie mediów.

Klicksafe.de bardzo skutecznie przeprowadził w niemieckich stacjach telewizyjnych oraz kinach kampanię z wykorzystaniem spotów telewizyjnych przygotowanych przez znaną agencję reklamową Ogilvy & Mather. Pierwszy klip, „Gdzie jest Klaus?" („Wo ist Klaus?"), ukazał się pod koniec roku 2005 i szybko zyskał powszechną aprobatę mediów, partnerów i odbiorców. Film w kilkuminutowym przekazie przedstawia szczególnie niebezpieczne aspekty związane z zawieraniem znajomości za pośrednictwem Sieci. Druga odsłona kampanii pod hasłem „W którym świecie żyjesz?", koncentrująca się na problemie uzależnienia od Internetu i komputera, została wyemitowana z okazji Dnia Bezpiecznego Internetu w 2008 roku i emitowana jest z dużym sukcesem do tej pory.

Spot „Gdzie jest Klaus?" cieszył się tak dużym zainteresowaniem wśród partnerów europejskich, że klicksafe we współpracy z agencją udostępnił materiał innym krajom do adaptacji językowej – dotychczas spot przetłumaczony został na język czeski, słoweński, hiszpański, niderlandzki, angielski.

Podobna sytuacja wystąpiła w przypadku polskiej kampanii „Dziecko w Sieci" prowadzonej pod hasłem „Nigdy nie wiadomo, kto jest po drugiej stronie". Spot telewizyjny i inne przekazy reklamowe kampanii, zdobyły uznanie m.in. w kilku krajach Europy Środkowo-Wschodniej, które podjęły się tłumaczenia tych materiałów na języki narodowe. Prawa do kampanii zostały przekazane organizacjom partnerskim na zasadach non-profit. Dotychczas kampania „Dziecko w Sieci" zrealizowana została na Łotwie, w Czechach, Bułgarii i Albanii.

W ostatnim czasie w swoich działaniach realizatorzy programu Safer Internet szczególną uwagę poświęcali niezmiernie popularnym wśród dzieci i młodzieży czatom oraz społecznościom internetowym. Duński oddział organizacji Save the Children aktywnie uczestniczy w programie **„Chat Check Badge"** skierowanym do właścicieli serwisów www, głównie tych oferujących czaty. Save the Children Denmark jest także członkiem utworzonej w roku 2007 rady „Chat Check". Aby zdobyć odznakę „Chat Check", właściciel strony www musi spełnić minimalne standardy dotyczące informacji i bezpieczeństwa online. Jedną z inicjatyw wspierających ten proces jest edukacja moderatorów nadzorujących serwisy internetowe. Organizacja Save the Children Denmark zainicjowała proces opracowywania kursów i materiałów szkoleniowych dla moderatorów - realizacja tego projektu rozpoczęła się w styczniu 2008, a pierwsza grupa moderatorów serwisów www przejdzie szkolenie w październiku tego roku.

V Przegląd polskich działań na rzecz bezpieczeństwa dzieci i młodzieży w Internecie

O zagrożeniach związanych z Siecią mówi się w Polsce stosunkowo od niedawna. Zagadnienia te w krótkim czasie stały się jednak powszechnie uznawane za ważną kwestię i wzbudzają coraz większe zainteresowanie mediów, organizacji społecznych, instytucji rządowych, rodziców, nauczycieli oraz samych zainteresowanych, czyli dzieci.

Jedną z pierwszych organizacji w Polsce, która zajęła się problematyką bezpieczeństwa dzieci w Internecie, była Fundacja Dzieci Niczyje. Przeprowadzone przez nią w 2002 r. badania zachowań dzieci w Sieci na próbie blisko 9 tys. internautów wykazały wysoki poziom ryzykownych zachować i niebezpiecznych doświadczeń dzieci *online*.

Niepokojące ustalenia badawcze, w zestawieniu ze znajomością doświadczeń krajów, w których Internet spopularyzował się kilka lat wcześniej, skłoniły Fundację Dzieci Niczyje do podjęcia działań mających na celu uświadomienie opinii społecznej zagrożeń związanych z Siecią i przygotowanie pola dla systemowych rozwiązań przeciwdziałających im. W lutym 2003 roku FDN wraz z partnerami z sektora organizacji pozarządowych oraz rządowych (m.in. MEN) rozpoczęła pierwszą ogólnopolską kampanię społeczną związana z problemem zagrożeń dzieci w Internecie w Internecie – „Dziecko w Sieci".

Pionierem w zakresie działań na rzecz bezpieczeństwa dzieci w Internecie była również Fundacja Kidprotect (obecnie: Kidprotect.pl), która uruchomiła pierwszy w Polsce hotline przyjmujący zgłoszenia dotyczące pornografii dziecięcej w Sieci oraz zajęła się działaniami edukacyjnymi adresowanymi przede wszystkim do przedstawicieli instytucji wymiaru sprawiedliwości i organów ścigania.

Ważnym momentem w krótkiej historii zapobiegania krzywdzeniu dzieci w Internecie w Polsce było wstąpienie Polski do Unii Europejskiej. W 2004 r. Polska, jako pierwszy z nowych krajów członkowskich, przystąpiła do realizacji programu Komisji Europejskiej Safer Internet Action Plan (SIAP). Narodowymi realizatorami programu zostały Fundacja Dzieci Niczyje oraz Naukowa i Internetowa Sieć Komputerowa (NASK). W ramach programu kontynuowana jest kampania „Dziecko w Sieci" wraz z szeregiem innowacyjnych propozycji edukacyjnych, na dużą skalę realizowane są szkolenia dla profesjonalistów oraz prowadzony jest *hotline* „Dyżurnet.pl", do którego internauci zgłaszać mogą nielegalne treści na które natknęli się w Sieci, oraz *helpline* „Helpline.org.pl", który udziela pomocy w sytuacjach zagrożenia dzieci w Sieci.

W działania na rzecz bezpieczeństwa dzieci w Internecie włączają się coraz chętniej firmy komercyjne, związane głównie z branżą telekomunikacyjną i branżą IT, realizując w ten sposób ideę społecznej odpowiedzialności biznesu. Najlepszym przykładem na takie działania jest konsekwentne zaangażowanie Grupy TP w kampanię „Dziecko w Sieci", projekt Helpline.org.pl oraz szereg innych działań realizowanych w ramach programu Safer Internet w Polsce. Widoczna jest również aktywność na tym polu firm Microsoft (seminaria, konferencje, wydawnictwa), UPC (program edukacyjny, wspieranie kampanii medialnych), Gemius SA (badania zagrożeń dla dzieci prowadzone non-profit) i innych.

Problematyka bezpieczeństwa dzieci w Internecie dostrzegana jest również coraz częściej przez instytucje rządowe. Godne odnotowania jest zaangażowanie w problematykę bezpieczeństwa dzieci w Internecie m.in. MSWiA (projekt zmiany ustawy o policji w celu skutecznej walki z pedofilią w Sieci), MEN (uwzględnienie tematyki bezpieczeństwa w Sieci w nowej podstawie programowej), Kancelaria Premiera (powołanie interdyscyplinarnego zespołu ds. bezpieczeństwa w Sieci).

5.1 Charakterystyka wybranych organizacji i instytucji realizujących działania na rzecz bezpieczeństwa dzieci w Internecie w Polsce

- **Fundacja Dzieci Niczyje**

Fundacja Dzieci Niczyje (FDN) jest organizacją pozarządową o charakterze non-profit, która od 1991 roku zajmuje się szeroko rozumianą pomocą dzieciom krzywdzonym, ich rodzinom i opiekunom. Od 2004 roku Fundacja realizuje ogólnopolską kampanię społeczną na rzecz bezpieczeństwa dzieci w Internecie „Dziecko w Sieci" oraz projekt edukacyjny dla dzieci „Sieciaki.pl". Od lutego 2007 roku FDN udziela pomocy młodym internautom w sytuacji zagrożenia w Sieci w ramach projektu Helpline.org.pl. Fundacja regularnie realizuje badania doświadczeń i postaw młodych internautów oraz ich rodziców. Pracownicy FDN prowadzą szkolenia z zakresu problematyki bezpieczeństwa dzieci w Internecie. Projekty fundacyjne związane z bezpieczeństwem dzieci w Internecie prowadzone są w ramach programu Akademia Bezpiecznego Internetu FDN. Od 2005 roku FDN jest koordynatorem projektu Awareness realizowanego wspólnie z NASK w ramach europejskiego projektu „Safer Internet". Głównym partnerem projektów FDN związanych z bezpieczeństwem dzieci w Sieci jest Fundacja Grupy TP.

- **Fundacja Grupy TP**

Fundacja Grupy TP (FGTP) powołana została grudniu 2005 roku przez Telekomunikację Polską i Orange w celu realizowania działań o charakterze społecznym, edukacyjnym i charytatywnym. Fundacja prowadzi między innymi program „Edukacja z Internetem TP" skierowany do szkół podstawowych, gimnazjalnych i ponad gimnazjalnych, którego celem jest promocja wykorzystania w edukacji technologii informacyjnych. W ramach programu realizowane są m.in. działania związanie z bezpieczeństwem dzieci *on-line*. FGTP jest głównym partnerem kampanii „Dziecko w Sieci" oraz edukacyjnego projektu „Sieciaki" Fundacji Dzieci Niczyje. Fundacja jest również głównym partnerem szeregu działań realizowanych w ramach programu Safer Internet w Polsce, jak Dzień Bezpiecznego Internetu, czy Międzynarodowa konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie". Wraz z Fundacja Dzieci Niczyje FDN realizuje projekt Helpline.org.pl oraz akcję „Sieciaki na wakacjach"

- **Fundacja Kidprotect.pl**

Fundacja Kidprotect.pl (wcześniej „Kidprotect") od 2002 roku specjalizuje się w ochronie dzieci korzystających z Internetu. Kidprotect.pl prowadzi hotline przyjmujący zgłoszenia pedofilii w Sieci, prowadzi szkolenia nauczycieli, rodziców i policjantów, opracowuje serwisy internetowe poświęcone problematyce bezpieczeństwa dzieci w Internecie (www.kidprotect.pl, www.bezpiecznyinternet.org). Od 2004 roku Fundacja Kidprotect.pl prowadzi kampanię społeczną „Stop pedofilom".

- **Komitet Konsultacyjny przy programie Safer Internet w Polsce**

Komitet Konsultacyjny został powołany w styczniu 2006 roku jako ciało doradcze, wspierające realizację programu Safer Internet w Polsce. Do zadań Komitetu należy pomoc w planowaniu działań na rzecz bezpieczeństwa dzieci w Internecie oraz ocena realizacji programu Safer Internet. W pracach Komitetu biorą udział przedstawiciele:

- Centralnego Ośrodka Doskonalenia Nauczycieli,
- Komendy Głównej Policji,
- Komendy Stołecznej Policji,
- Ministerstwa Edukacji i Nauki,
- Ministerstwa Nauki i Informatyzacji,
- Ministerstwa Sprawiedliwości,

- Ministerstwa Spraw Wewnętrznych i Administracji,
- Ministerstwa Pracy i Polityki Społecznej,
- Polskiej Izby Informatyki i Telekomunikacji,
- Rzecznika Praw Dziecka,
- Polskiego Komitetu ds. UNESCO,
- Urzędu Ochrony Konkurencji i Konsumentów,
- Związku Producentów Audio-Video.

- **Naukowa i Akademicka Sieć Komputerowa**

NASK jest jednostką badawczo-rozwojową, działającą na rynku polskim od grudnia 1993 roku. NASK jest pionierem polskiego Internetu i jednym z wiodących w kraju operatorów teleinformatycznych. W strukturze NASK działa zespół CERT Polska – Computer Emergency Response Team, zajmujący się rejestracją, obsługą i klasyfikacją zdarzeń naruszających bezpieczeństwo Sieci. Zespół włącza się w międzynarodowe inicjatywy na rzecz podwyższania bezpieczeństwa sieci i systemów IT, m. in. aktywnie współpracuje z europejską agencją ENISA (European Network and Information Security Agency). Od 2005 roku NASK wraz z Fundacją Dzieci Niczyje realizuje w Polsce program Komisji Europejskiej „Safer Internet". W ramach programu NASK prowadzi projekt Dyżurnet.pl - hotline zajmujący się obsługą zgłoszeń nielegalnych treści w Internecie, oraz uczestniczy w realizacji projektu Awareness, w ramach którego realizowane są działania edukacyjne na rzecz bezpieczeństwa dzieci w Internecie.

5.2 Charakterystyka wybranych projektów na rzecz bezpieczeństwa dzieci w Internecie

- **Kampania „Dziecko w Sieci"**

Ogólnopolska kampania społeczna „Dziecko w Sieci" zainicjowana została przez Fundację Dzieci Niczyje w lutym 2004 roku. Podstawowym jej celem było zwrócenie uwagi dorosłych i dzieci na zagrożenia związane z aktywnością pedofilów w Sieci oraz edukacja w zakresie bezpiecznego korzystania z Internetu. W ramach kampanii „Dziecko w Sieci" prowadzone są badania poświęcone zagrożeniom dzieci w Internecie. Na podstawie dostępnej wiedzy, wyników badań oraz doświadczeń pracowników FDN wypracowywane są przekazy medialne oraz projekty edukacyjne poświęcone bezpieczeństwu najmłodszych Internautów. Ważnym elementem kampanii „Dziecko w Sieci" są również szkolenia dla profesjonalistów pracujących z dziećmi oraz zaangażowanych w zwalczanie przestępczości wobec najmłodszych Internautów. Od stycznia 2005 kampania realizowana jest w ramach programu Komisji Europejskiej „Safer Internet" jako kompleksowy projekt edukacyjny na

rzecz bezpieczeństwa dzieci i młodzieży w Sieci. Głównym partnerem kampanii jest Fundacja Grupy TP (FGTP).

„Nigdy nie wiadomo, kto jest po drugiej stronie"

Kampania medialna prowadzona pod hasłem „Nigdy nie wiadomo, kto jest po drugiej stronie" to pierwszy projekt zrealizowany w ramach kampanii „Dziecko w Sieci". Akcja poświęcona została problemowi uwodzenia dzieci w Internecie i rozpoczęła w Polsce dyskusję na temat tego problemu. Dzięki dużemu zaangażowaniu mediów kampania uzyskała widoczność na poziome ponad 70% ogółu Polaków (Gemius 2005). W ramach kampanii od lutego do czerwca 2004 roku prezentowane były reklamy telewizyjne, radiowe, prasowe oraz zewnętrzne. Do akcji włączyło się, m.in. 8 ogólnopolskich stacji telewizyjnych, 19 stacji radiowych, 33 tytuły prasowe (ponad 120 publikacji reklamy), oraz blisko 200 portali i serwisów internetowych. Reklama zewnętrzna (bilboardy oraz plakaty przystankowe) eksponowana była w 18 największych miastach Polski.

Spot telewizyjny wykorzystany w kampanii prezentujący rozmowę na czacie pomiędzy dziewczynką (Ania) i dorosłym mężczyzną podającym się za jej rówieśnika (Wojtek) do dzisiaj wykorzystywany w materiałach telewizyjnych dotyczących przypadków pedofilii w Internecie.
Kampania „Dziecko w Sieci" została przetłumaczona i zrealizowana w Bułgarii, na Słowacji, oraz na Łotwie.

„Internet to okno na świat. Cały świat."

Pod hasłem „Internet to okno na świat. Cały świat" od września 2007 roku prowadzona była akcja medialna której celem było zwrócenie uwagi dorosłych na niebezpieczne treści, na jakie mogą natrafić ich dzieci podczas samotnego korzystania z Internetu (pornografia, sceny drastyczne, ksenofobia, rasizm). Kampania

W ramach kampanii, realizowanej była przez FDN oraz NASK w ramach programu „Safer Internet", przygotowane zostały dwa spoty telewizyjne, dwa spoty radiowe, reklama prasowa (2 projekty) oraz reklama zewnętrzna (citylight). Do akcji włączyło się 8 stacji telewizyjnych (w tym wszystkie kanały telewizji publicznej, 22 rozgłośnie radiowe, 16 dzienników i magazynów. Reklama zewnętrzna prezentowana była w Warszawie, Krakowie, Łodzi, Poznaniu i Toruniu. Kampania została nagrodzona na licznych przeglądach reklamy w kraju i za granicą.

„Stop cyberprzemocy”

Pod hasłem „Stop Cyberprzemocy” od stycznia 2008 roku realizowane są działania medialne i edukacyjne poświęcone problemowi przemocy rówieśniczej z użyciem Internetu i telefonów komórkowych. Kampania poprzedzona została ogólnopolskimi badaniami skali problemu wśród dzieci korzystających z Internetu oraz analizą przypadków zgłaszanych do Helpline.org.pl

W ramach akcji przygotowano spot telewizyjny i radiowy oraz reklamy prasowe poświęcone problemowi cyberprzemocy. W pierwszym półroczu 2008 roku reklamy prezentowane były w kilkudziesięciu ogólnopolskich i lokalnych stacjach telewizyjnych oraz tytułach prasowych. NA potrzeby kampanii „Stop Cyberprzemocy” przygotowany został również 2 minutowy film szkoleniowy, który wraz ze scenariuszami zajęć dotyczących problemu przemocy rówieśniczej z użyciem nowych technologii jest dystrybuowany w szkołach gimnazjalnych w całej Polsce. Przekazy akcji „Stop Cyberprzemocy" promują wśród dzieci, młodzieży, nauczycieli i rodziców ofertę pomocową helpline.org.pl.

- **Dzień Bezpiecznego Internetu**

Dzień Bezpiecznego Internetu (*Safer Internet Day*) obchodzony jest od 2004 roku z inicjatywy Komisji Europejskiej. Akcja ma na celu zwrócenie uwagi opinii publicznej na kwestię bezpiecznego korzystania przez dzieci i młodzież z zasobów internetowych. Organizacja DBI jest jednym z zadań narodowych realizatorów programu Safer Internet (FDN, NASK). W Polsce Dzień Bezpiecznego Internetu obchodzony był po raz pierwszy 8 lutego 2005 roku. Z tej okazji pod adresem www.dbi.pl opublikowany został serwis internetowy, w którym zaprezentowana została idea DBI oraz wskazówki dla lokalnych organizatorów jak włączyć się w jego obchody. Organizatorzy zachęcali w nim m.in. lokalne organizacje społeczne, szkoły, domy kultury, władze lokalne, właścicieli kawiarni internetowych do realizacji przedsięwzięć na rzecz bezpieczeństwa w Sieci. W serwisie udostępniono również materiały pomocnicze dla lokalnych organizatorów Dnia Bezpiecznego Internetu. Podobne zasady towarzysza kolejnym obchodom DBI organizowanym corocznie w pierwszych dniach lutego Z okazji DBI Fundacja Dzieci Niczyje wraz z NASK organizują w Bibliotece Uniwersyteckiej w Warszawie konferencje dla przedstawicieli mediów i partnerów programu „Safer Internet" w Polsce, podczas których prezentowany jest przebieg DBI, osiągnięcia i plany programu „Safer Internet" w Polsce oraz inne inicjatywy związane z bezpieczeństwem w Internecie. Głównym partnerem obchodów DBI w Polsce jest Fundacja Grupy TP.

- **Ogólnopolska Koalicja na rzecz Bezpiecznego Internetu (OKBI)**

Powołana w lutym 2006 roku Ogólnopolska Koalicja na rzecz Bezpiecznego Internetu jest platformą współpracy instytucji rządowych, pozarządowych, szkół i innych placówek oświatowych oraz firm komercyjnych na rzecz bezpieczeństwa dzieci i młodzieży w Internecie. Koalicja działa w ramach projektu Safer Internet w Polsce i koordynowana są przez FDN i NASK – narodowych realizatorów projektu.

Główne cele Koalicji to:

• Podniesienie świadomości społecznej na temat zagrożeń w Internecie;

• Wymiana doświadczeń w zakresie działań na rzecz bezpieczeństwa w Internecie;

• Nagłaśnianie problemów związanych z zagrożeniami internetowymi;

• Współpraca przy realizacji inicjatyw mających na celu podniesienie poziomu bezpieczeństwa Internautów;

• Dystrybucja informacji o działaniach podejmowanych w Polsce i Europie w ramach programu *Safer Internet*.

Organizacje i instytucie zainteresowanie problematyką bezpieczeństwa dzieci *on-line* mogą przystąpić do OKBI wypełniając odpowiedni formularz w serwisie **www.saferinternet.pl**. Na stronie projektu Safer Internet członkowie Koalicji mają też możliwość promowania swoich inicjatyw na rzecz bezpieczeństwa w Sieci.

- **Kampania „Stop pedofilom"**

Kampania „Stop Pedofilom" prowadzona od 2004 roku przez fundację Kidprotect.pl poświęcona jest zjawiskom prostytucji dziecięcej, uwodzenia dzieci i pornografii dziecięcej. Część przekazów kampanii „Stop Pedofilom" koncentruje się na problemie pedofilii w Internecie. W kolejnych odsłonach kampanii nośnikami przekazów reklamowych były kartki pocztowe, reklamy prasowe, reklamy telewizyjne i radiowe. Kampania ma na celu uświadomienie dorosłym odbiorcom występowania zagrożeń związanych z wykorzystywaniem seksualnym dzieci oraz powinność informowania odpowiednich służb o przypadkach pedofilii. Hasła wykorzystywane w kampanii to „Stop pedofilom", „Milczenie nie jest złotem".

Przekazy kampanii „Stop Pedofilom" odsyłają odbiorców do serwisu internetowego www.kidprotect.pl, gdzie obok treści związanych z problemem pedofilii znajduje się formularz, za którego pośrednictwem zgłaszać można fundacji Kidprotect.pl przypadki wykorzystywania seksualnego dzieci.

- **Sieciaki.pl**

Sieciaki.pl to projekt edukacyjny adresowany do dzieci, prowadzony od lutego 2005 roku przez Fundację Dzieci Niczyje. Jego podstawowym elementem jest atrakcyjny serwis internetowy www.sieciaki.pl poświęcony bezpieczeństwu w Internecie, który angażuje dzieci w liczne gry,

zabawy i konkursy. Do września 2008 roku w serwisie zarejestrowało się blisko 90 tys. użytkowników.

W ramach programu organizowane są również spotkania z dziećmi, imprezy plenerowe, koncerty oraz zajęcia edukacyjne. Przygotowywane są filmy, kreskówki, piosenki, teledyski i liczne materiały multimedialne.

Projekt Sieciaki.pl ma na celu:

- edukację dzieci w zakresie bezpieczeństwa w Internecie,
- edukację w zakresie posługiwania się Internetem,
- promocję bezpiecznych zastosowań Sieci,
- certyfikowanie i promocję bezpiecznych stron i serwisów internetowych.

W ramach projektu „Sieciaki.pl" corocznie, w Warszawie i wybranych miejscowościach wypoczynkowych, pod hasłem „Sieciaki na wakacjach" organizowana jest seria pikników internetowych. W plenerowych zajęciach edukacyjnych każdego roku bierze udział kilka tysięcy dzieci. Głównym Partnerem projektu jest Fundacja Grupy TP.

- **Dyżurnet.pl**

Dyżurnet.pl jest punktem kontaktowym, który przyjmuje zgłoszenia dotyczące nielegalnych treści znalezionych w Internecie. Powołany został w 2006 roku przez NASK i funkcjonuje w ramach programu Safer Internet w Polsce. Do zadań Dyżurnet.pl należy m.in. analiza treści wskazanych przez użytkowników, wykonanie dokumentacji technicznych, przesłanie informacji do policji, prokuratury, administratorów serwisów internetowych, czy też zagranicznych punktów kontaktowych. Dyżurnet.pl jest zrzeszony w międzynarodowym stowarzyszeniu helplineów INHOPE.

Nielegalne treści znalezione w Internecie można zgłaszać do Dyzurnet.pl za pomocą formularza na stronie www.dyzurnet.pl lub nagrywając wiadomość pod numerem 0801 615 005.

- **Helpline.org.pl**

Helpline.org.pl jest wspólnym projektem Fundacji Dzieci Niczyje i Fundacji Grupy TP, współfinansowanym przez Komisję Europejską w ramach programu Safer Internet Plus. Helpline uruchomiony został w lutym 2007 roku. Jego celem jest pomoc dzieciom i młodzieży w sytuacjach zagrożenia w Internecie. Konsultanci Helpline.org.pl udzielają także porad rodzicom, opiekunom i osobom pracującym zawodowo z dziećmi i młodzieżą.

Helpline.org.pl działa w dni powszednie w godzinach od 11 do 16. Kontakt z konsultantami jest możliwy pod bezpłatnym numerem telefonu 0 800 100 100, za pośrednictwem livechat'u z poziomu strony www.helpline.org.pl, oraz za pomocą e-maila: helpline@helpline.org.pl.

Helpline.org.pl zrzeszony jest w międzynarodowym stowarzyszeniu Child Helpline International.

- **Konferencja „Bezpieczeństwo dzieci i młodzieży w Internecie"**

Międzynarodowe konferencje „Bezpieczeństwo dzieci i młodzieży w Internecie" organizowane są corocznie w Warszawie przez Fundację Dzieci Niczyje oraz Naukową i Akademicką Sieć Komputerową, we współpracy z partnerami zagranicznymi realizującymi program Komisji Europejskiej Safer Internet Plus. Pierwsza konferencja z tego cyklu zorganizowana została w sierpniu 2007 roku. Kolejna odbywa się we wrześniu 2008 roku. Dwie kolejne konferencje zaplanowane zostały na wrzesień 2009 i 2010 r.

Konferencje poświęcone są szerokiemu spektrum zagadnień związanych z bezpieczeństwem dzieci i młodzieży w Internecie. Uczestniczą w nich przedstawiciele sektora edukacyjnego, organizacji pozarządowych, branży internetowej, instytucji wymiaru sprawiedliwości oraz organów ścigania.

Celem konferencji jest przekazywanie uczestnikom najnowszej wiedzy zarówno w zakresie działań edukacyjnych, jak również zwalczania nielegalnych treści w Sieci. W programie konferencji znajdą się wykłady oraz warsztaty prowadzone przez uznanych specjalistów z zagranicznych i krajowych organizacji zajmujących się bezpieczeństwem dzieci *on-line.*

- **Akademia e-Bezpieczeństwa UPC**

Program edukacyjny Akademia e-Bezpieczeństwa UPC adresowany jest do całych rodzin, zarówno rodziców, jak i dzieci i ma ca celu dostarczenie wiedzy i umiejętności pomocnych we wspólnym przygotowaniu się do korzystania z komputera i Internetu. Elementami programu Akademia e-Bezpieczeństwa UPC są warsztaty dla rodziców, strona internetowa www.upclive.pl/dzieci oraz specjalny podręcznik „Bezpieczeństwo w sieci – elementarz dla całej rodziny". Został on wydany w lutym 2008 r. przez UPC oraz organizację Insafe powołaną przez Komisję Europejską i działającą na rzecz bezpieczeństwa w Internecie. Publikacja jest przeznaczona dla dzieci w wieku od 6 do 12 lat oraz ich rodziców. Ma im pomóc we wspólnym przygotowaniu się do korzystania z komputera i Internetu. Przewodnik dystrybuowany jest w wersji papierowe oraz można go również pobrać *online* pod adresem www.upclive.pl/dzieci.

- **TP CERT**

TP CERT jest zespołem reagującym na pojawiające się zagrożenia w sieci, którego celem działań jest pomoc społeczności internetowej TP w wykrywaniu, rozwiązywaniu i zapobieganiu powstawania incydentów bezpieczeństwa.

Telekomunikacja Polska dbając o bezpieczeństwo użytkowników korzystających z sieci powołała w 1997 roku zespół reagujący na przypadki zagrożeń bezpieczeństwa teleinformatycznego (ICT - Information and Comunication Technology), zaobserwowane lub zgłoszone przez użytkowników sieci - CSIRT (Computer Security Incident Response Team). Od roku 2006 zespół działa pod nazwą TP CERT (Computer Emergency Response Team).

Działalność TP CERT polega na reagowaniu na pojawiające się incydenty bezpieczeństwa komputerowego oraz zapobieganiu ich powstawania i obejmuje swym zakresem użytkowników internetu, których systemy (komputery) przyłączone są do sieci TP

Cele działalności:

- pomoc społeczności internetowej TP we wprowadzaniu proaktywnych środków redukujących ryzyko wystąpienia incydentów związanych z zagrożeniem i/lub naruszeniem bezpieczeństwa sieciowego, w szczególności: alarmowanie i informowanie użytkowników o cyberzagrożeniach

- pomoc społeczności internetowej TP w reagowaniu na przypadki, które się zdarzyły (lub mają miejsce), w szczególności: zapewnienie jednego zaufanego punktu kontaktowego dla użytkowników sieci i koordynacja obsługi incydentów

Więcej informacji na www.tp.pl/cert

Fundacja Dzieci Niczyje -Istnieje od 1991 roku, jest organizacją pozarządową o charakterze non-profit, której celem jest ochrona dzieci przed krzywdzeniem oraz pomoc dzieciom krzywdzonym, ich rodzinom i opiekunom. Placówki prowadzone przez Fundację udzielają pomoc psychologiczną, medyczną i prawną ofiarom krzywdzenia i ich opiekunom. FDN działa na rzecz poprawy sytuacji dzieci uczestniczących w procedurach prawnych w charakterze świadków. Prowadzi programy profilaktyki krzywdzenia dzieci przez dorosłych oraz rówieśników, organizuje specjalistyczne szkolenia z zakresu problematyki dziecka krzywdzonego dla różnych grup profesjonalnych oraz zespołów interdyscyplinarnych. Prowadzi badania i analizy poszerzające wiedzę o problemie oraz stanowiące podstawę projektowanych działań. www.fdn.pl

Interactive Advertising Bureau Polska (IAB) – Związek Pracodawców Branży Internetowej, wśród członków stowarzyszenia znajdują się portale i wortale internetowe, sieci reklamowe, agencje interaktywne. Jednym z ważniejszych zadań stowarzyszenia jest szeroko pojęta edukacja rynku w zakresie metod wykorzystania Internetu. www.iabpolska.pl

Digital One (Grupa Euro RSCG) – Strategiczna agencja interaktywna specjalizująca się w Digital Experience, koncentrująca się na tworzeniu strategii budowania wizerunku marki w obszarze nowych mediów, przy wykorzystaniu innowacyjnych technologii i narzędzi e-marketingwych. W swoim portfolio agencja posiada wiele serwisów dla dzieci i młodzieży w tym: *Klub Mamby* (Storck), *Bądź MAX* (Pepsi-Cola General Bottlers Polska), *Pomarańczowa odyseja* (dla marki Mirinda), *Wirtualny Stadion* (TP), strony produktów *Action Man, HitClips, Pokemon i Poo-Chi* (Hasbro). www.digitalone.pl

Dyżurnet.pl - punkt kontaktowy (Hotline) przyjmujący zgłoszenia dotyczące nielegalnych treści w Internecie. Do jego zadań należy m.in. analiza treści wskazanych przez użytkowników, przesłanie informacji do policji, prokuratury, administratorów serwisów internetowych czy też zagranicznych punktów kontaktowych zrzeszonych w INHOPE. Dyżurnet.pl został utworzony przez Naukową i Akademicką Sieć Komputerową w porozumieniu z Komisją Europejską w ramach akcji Safer Internet Action Plan. www.dyzurnet.pl

Bebo.com – jedna z największych społecznych sieci medialnych na świecie, dająca m.in. możliwość przeglądania, tworzenia, wyszukiwania i dzielenia się treściami generowanymi przez profesjonalistów oraz samych użytkowników. Zrzesza 11,4 mln unikalnych użytkowników w Wielkiej Brytanii, a łącznie ponad 40 milionów zarejestrowanych użytkowników na całym świecie. www.bebo.com