Warszawa, 2 kwietnia 2012 r

Ministerstwo Administracji i Cyfryzacji
Departament Społeczeństwa Informacyjnego
00-950 Warszawa, ul. Domaniewska 36/38

Ministerstwo Administracji i Cyfryzacji zaprosiło do składania uwag dotyczących **Komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów** – "Ocena okresowa wieloletniego unijnego programu ochrony dzieci korzystających z Internetu oraz innych technologii komunikacyjnych COM(2012) 033" (dalej: **Komunikat**). Uwagi te mają zostać wykorzystane w trakcie przygotowywania stanowiska rządu odnośnie Komunikatu.

W związku z przedstawionymi w Komunikacie wynikami oceny okresowej programu „Bezpieczniejszy Internet" na lata 2009-2013 **Fundacja Kidprotect.pl, Fundacja Panoptykon, Stowarzyszenie ISOC Polska, Fundacja Nowoczesna Polska, Fundacja Instytut Rozwoju Regionalnego oraz Fundacja Wolnego i Otwartego Oprogramowania** ustosunkowują się do przedstawionych w zawiadomieniu MAiC pytań.

Na wstępie podkreślamy, że uważamy za niezbędne poszerzenie perspektywy, w jakiej postrzega się program "Bezpieczniejszy Internet". Niestety w Komunikacie zostały właściwie pominięte wnioski z Projektu EU Kids Online II (jedynie się o nich wspomina). Tymczasem w naszej opinii wnioski te są kluczowe, jeśli chodzi o zapewnienie właściwej ochrony najmłodszych użytkowników sieci. W powstałych w ramach projektu opracowaniach zawarta jest wiedza o doświadczeniach dzieci i rodziców odnośnie ryzyk związanych z korzystaniem przez dzieci z sieci i radzeniu sobie z tymi zagrożeniami. Naszym zdaniem należy skorzystać z zawartej w **EU Kids Online II** oceny sytuacji oraz końcowych rekomendacji. Z tego powodu przedstawiliśmy je w zarysie po ustosunkowaniu się do przedłożonych przez MAiC pytań[1].

[1] Jeśli Komisja nie zgadza się z wnioskami jakie wynikają z zamówionego przez nią badania, to powinna przynajmniej wyjaśnić z którymi wnioskami i dlaczego się nie zgadza.

1. Czy Państwa zdaniem program „Bezpieczniejszy Internet" w stopniu wystarczającym odpowiada potrzebom w dziedzinie poprawy bezpieczeństwa korzystania z Internetu?

Program „Bezpieczniejszy Internet" jest potrzebny z punktu widzenia troski o bezpieczeństwo, szczególnie najmłodszych użytkowników Internetu. Jednak w naszej ocenie nie odpowiada on potrzebom w zakresie poprawy bezpieczeństwa korzystania z Internetu w stopniu wystarczającym.

Po pierwsze, w realizacji programu na polskim gruncie hasło "Bezpieczniejszy Internet" zostało sprowadzone do problematyki dziecięcej, która w oczywisty sposób jest istotna, ale nie stanowi jedynej grupy problemów związanych z cyberbezpieczeństwem. W ramach działań objętych programem brakuje wielu obszarów i aspektów bezpieczeństwa.

Po drugie, program „Bezpieczniejszy Internet" koncentruje się na **anachronicznych** – w naszej opinii – **formach profilaktycznych** (plakaty, ulotki, pogadanki, konferencje), podczas gdy - przynajmniej w stosunku do dzieci i młodzieży – skuteczniejsze są działania, w których angażuje się rówieśników. Ma to miejsce szczególnie w przypadku wykorzystania różnych form wychowania przez sztukę.

Po trzecie, brakuje w nim działań systemowych np. na rzecz **wprowadzenia edukacji medialnej i informacyjnej** w systemie oświaty. Warto zwrócić uwagę, że w tej dziedzinie mamy w Polsce spore problemy: edukacja medialna znajduje się w kompetencjach wielu różnych organów administracji publicznej, co powoduje rozmycie odpowiedzialności, brakuje jasnego planu działania w tej sferze, w szczególności niejasne są zamierzenia MEN. Szczegółowa analiza stanu edukacji medialnej i informacyjnej w Polsce dostępna jest w raporcie "Cyfrowa Przyszłość" Fundacji Nowoczesna Polska[2].

Potrzeby w dziedzinie poprawy bezpieczeństwa korzystania z Internetu wykraczają daleko poza możliwości podmiotów prywatnych (jak organizacje zrzeszone w sieci INHOPE). Potrzebne są również konkretne i odpowiednio zsynchronizowane działania podejmowane przez władze publiczne. W szczególności:

(1) **Państwa Unii Europejskiej powinny podjąć zdecydowane kroki w celu wzmocnienia współpracy międzypaństwowej**, w tym z państwami trzecimi, w celu skutecznego i szybkiego usuwania nielegalnych treści z Internetu. Priorytetem musi być usunięcie systemowych barier w komunikacji i współpracy z organami ścigania z państw trzecich, które powodują, że nie są przesyłane zawiadomienia o łamaniu prawa do odpowiednich organów innych państw, a ewentualna reakcja jest niewystarczająco sprawna i szybka (współpraca ta mogłaby obejmować np. stworzenie punktów kontaktowych dla odpowiednich instytucji za granicą).

[2] Raport dostępny pod adresem

http://nowoczesnapolska.org.pl/2012/01/20/edukacja-medialna-i-informacyjna-raport-otwarcia/.

(2) Należy stworzyć europejski system corocznego raportowania o postępach w usuwaniu nielegalnych treści z Internetu. Konsekwentne stosowanie tego środka umożliwi instytucjom Unii Europejskiej ocenę sukcesów i porażek poszczególnych państw członkowskich na płaszczyźnie krajowej i międzynarodowej, co z kolei pomoże w promowaniu najlepszych praktyk i zagwarantowaniu, że podejmowane są maksymalne starania na polu wykrywania przestępstw, ścigania sprawców i identyfikowania ofiar.

2. Jak oceniają Państwo wyniki przeprowadzonej przez Komisję Europejską okresowej oceny programu pod kątem Państwa własnych obserwacji i doświadczeń w tej dziedzinie? Na co Komisja Europejska powinna zwrócić uwagę przy przeprowadzaniu końcowej oceny programu?

W naszej opinii Komisja Europejska, dokonując okresowej oceny programu „Bezpieczniejszy Internet", powinna przede wszystkim zwrócić uwagę na zagrożenia dla praworządności i podstawowych praw obywateli-użytkowników Internetu związane z powierzeniem podmiotom prywatnym niektórych kompetencji właściwych dla organów egzekwowania prawa. Komisja Europejska powinna zwrócić szczególną uwagę na sposób realizacji i efekty programu w zakresie następujących celów:

- udostępnienie obywatelom sieci punktów kontaktowych, w których można zgłaszać nielegalne i szkodliwe treści oraz zachowania, w szczególności materiały przedstawiające wykorzystywanie dzieci, materiały mające na celu nagabywanie dzieci dla celów seksualnych oraz cyberprzemoc;
- większy nacisk w programach edukacyjnych, skierowanych nie tylko na uświadomienie możliwych sposobów obrony przed prześladowanymi ze strony rówieśników, ale również z uświadomieniem ponoszonej odpowiedzialności prawnej z tego powodu zachowań prześladowczych.
- angażowanie dzieci w tworzenie bezpiecznego środowiska w Internecie.

Okresowej ocenie Komisji Europejskiej powinny być poddane działania podejmowane zarówno przez organizacje zrzeszone w sieci INHOPE, jak i dostawców usług internetowych. Po pierwsze, Komisja powinna przeanalizować efektywność komunikacji pomiędzy organizacjami prowadzącymi punkty kontaktowe a organami egzekwowania prawa (np. Policją), aby zweryfikować trafność zgłoszeń i skuteczność ich realizacji. Po drugie, Komisja powinna zweryfikować praktyki wszelkich podmiotów prywatnych zaangażowanych w realizację programu „Bezpieczniejszy Internet" – w tym inicjatywy samoregulacyjne – z punktu widzenia ich zgodności z obowiązującym prawem i ryzyka naruszeń takich praw podstawowych, jak prawo do prywatności, wolność słowa czy prawo do informacji (*vide* poniżej). Po trzecie, analizie powinna podlegać współpraca między uprawnionymi organami państw członkowskich między sobą oraz na styku z państwami trzecimi.

W tym kontekście nasz niepokój wzbudził np. ten fragment Komunikatu:

„W przypadku stwierdzenia nielegalnych treści, linia interwencyjna skieruje sprawę do odpowiednich organów wymiaru sprawiedliwości w kraju lub do dostawcy usług internetowych z żądaniem usunięcia treści albo do członka sieci Międzynarodowego Stowarzyszenia Internetowych Numerów Interwencyjnych (INHOPE), jeśli treści są zamieszczone na serwerach zagranicznych".

Nie jest dla nas jasne, czy i w jakim stopniu podmioty prywatne zaangażowane w realizację programu „Bezpieczniejszy Internet" mogą się dopuszczać takich praktyk, jak arbitralne usuwanie lub blokowanie treści bez angażowania organów wymiaru sprawiedliwości. Okresowa ocena Komisji Europejskiej powinna rozwiać wszelkie tego typu wątpliwości i pozwolić na sformułowanie wniosków, z których wynikną zasady, których uczestnicy programu powinni bezwzględnie przestrzegać.

Walka z nielegalnymi treściami umieszczanymi w Internecie nieodzownie wiąże się z rozstrzyganiem kolizji praw podstawowych, takich tak prawo do prywatności czy obowiązek poszanowania godności człowieka z jednej strony, a wolność wypowiedzi czy prawa do dostępu do informacji z drugiej strony. Dopuszczenie samoregulacji w tym newralgicznym obszarze oznaczałoby przekazanie prywatnym podmiotom uprawnień, jakie powinny być zarezerwowane dla organów wymiaru sprawiedliwości. Uważamy, że podmioty sektora prywatnego zajmujące się wspieraniem zwalczania przestępczości w sieci **powinny korzystać z uprawnień przysługujących każdemu z obywateli** i nie powinny posiadać specjalnych prerogatyw czy korzystać ze szczególnego zwolnienia od odpowiedzialności.

W tym kontekście przypominamy również, że blokowanie (jakichkolwiek) stron lub ograniczanie dostępu do zasobów w Internecie stanowi zagrożenie dla wolności słowa. Nie jest możliwe zastosowanie tego środka z „laserową precyzją" jedynie do treści, które bezdyskusyjnie uznamy za nielegalne. Ofiarą cenzury muszą paść także treści legalne, np. całe serwisy służące do hostingu materiałów video, encyklopedie czy fora internetowe. Po pierwsze dlatego, że wyznaczenie twardej granicy pomiędzy nielegalną pornografią dziecięcą a legalną pornografią czy erotyką jest niemożliwe. Po drugie dlatego, że nawet bezdyskusyjne treści są zwykle przechowywane na stronach razem z legalnymi, które blokujemy „przy okazji". Wreszcie, samo wprowadzenie infrastruktury cenzurującej – czyli stworzenie technicznych możliwości filtrowania i blokowania treści w Internecie na poziomie podmiotów, które tę treść dostarczają zwykłym użytkownikom – stanowi istotne ograniczenie praw obywatelskich i generuje poważne zagrożenia dla wolności słowa i ochrony prywatności użytkowników Internetu.

3. Czy Państwa zdaniem trzeba będzie kontynuować program po 2013 roku? Jakie zmiany i ulepszenia powinny być wprowadzone w kolejnej edycji programu?

Stoimy na stanowisku, że program „Bezpieczniejszy Internet" powinien być kontynuowany po 2013 roku. Troska o bezpieczeństwo, w tym ochrona przed zagrożeniami wynikającymi z korzystania z nowoczesnych technologii komunikacyjnych wymaga podejmowania działań nieustających. Działania te powinny mieć charakter systemowy i systematyczny. Należy jednak rozważyć wprowadzenie następujących zmian:

(1) Obecnie program „Bezpieczniejszy Internet" na gruncie polskim realizowany jest przez konsorcjum NASK i Fundacji Dzieci Niczyje, czyli instytucji o bliżej nieokreślonym statusie oraz organizacji pozarządowej.

Pożądanym rozwiązaniem byłoby podanie programu pod nadzór instytucji publicznych: Ministerstwa Edukacji Narodowej i Ministerstwa Spraw Wewnętrznych. W ramach instytucji

publicznych powinny być oceniane wnioski i przyznawane dofinansowania. Rozwiązanie to jest uzasadnione faktem, że resort edukacji odpowiada za tworzenie warunków dla właściwego przebiegu procesów wychowawczych, a resort spraw wewnętrznych odpowiada za działania na rzecz bezpieczeństwa, a jednocześnie ma ogromne doświadczenie w realizacji programów profilaktycznych.

(2) Program „Bezpieczniejszy Internet" powinien w większym stopniu otworzyć się na problematykę bezpieczeństwa dorosłych, w tym również seniorów. Łącznie z przygotowaniem programów edukacyjnych skierowanych do tych środowisk.

(3) Program „Bezpieczniejszy Internet" powinien w równym stopniu uwzględniać wątki technologiczne, prawne i wychowawcze (np. nauczanie wartości w ramach działań profilaktycznych dotyczących dzieci i młodzieży).

(4) Elementem założeń pryncypialnych programu „Bezpieczniejszy Internet" powinny być: zasada neutralności sieci, promocja otwartych zasobów edukacyjnych oraz poszanowanie praw podstawowych.

(5) Program „Bezpieczniejszy Internet" nie powinien promować inicjatyw samoregulacyjnych zakładających blokowanie stron internetowych na poziomie systemu DNS.

* * *

Wyniki z europejskich badań nad używaniem Internetu przez dzieci[3]

Przyczyną zmian sytuacji dzieci są możliwości jakie daje wzrost gospodarczy i postęp technologiczny. Wychodząc z obserwacji długotrwałych trendów,można zauważyć tendencję do indywidualizacji mediów[4], która jest długookresowym procesem wynikającym z zapotrzebowania i zmieniającej się oferty jakiej dostarcza rozwój techniki[5]. Obecnie normą staje się sytuacja, w której dziecko całkiem samodzielnie ze swojego pokoju komunikuje się ze znajomymi z serwisu społecznościowego. **Osoby dorosłe mają coraz mniejszy wgląd na to, jak dzieci korzystają z Internetu**.

Właśnie dla rozpoznania tej rzeczywistości i stworzenia empirycznych podstaw dla kształtowania polityki w zakresie bezpieczeństwa w Internecie przeprowadzono badanie kwestionariuszowe „Dzieci Unii Europejskiej w sieci" (EU Kids Online).

---

[3] Określenie „dzieci" obejmuje korzystające z Internetu w Europie dzieci i młodzież w wieku od 9 do 16 lat.

[4] Już pojawienie się domowego kina w postaci czarno-białego telewizora było etapem w procesie indywidualizacji. Jest to proces ciągły. Z czasem pojawiły się przenośne odtwarzacze i słuchawki – stwarzające możliwość indywidualnego słuchania muzyki – oraz telewizory w sypialniach. Rodzinny stacjonarny PC jest wypierany przez osobiste laptopy.

[5] Livingstone, Sonia (2010), *Youthful participation: what have we learned, what shall we ask next? In: First Annual Digital Media and Learning Conference: Diversifying Participation*, 18-20 February 2010, University of California, San Diego, La Jolla, California, USA [http://eprints.lse.ac.uk/27219/].

Wiosną i latem 2010 roku w 25 krajach Unii Europejskiej przeprowadzono wywiady z losowo dobraną próbą 25.142 korzystających z Internetu dzieci w wieku od 9 do 16 lat; uzupełniając je o dodatkowe przepytani po jednym z rodziców każdego badanego dziecka.

W kwestionariuszach pytano o takie zagrożenia związane z korzystaniem z Internetu, jak: pornografia, znęcanie się i dokuczanie innym [ang. *bullying*], otrzymywanie wiadomości o treści związanej z seksem, nawiązywanie kontaktów *online* z osobami nieznanymi osobiście, spotkania twarzą w twarz z osobami poznanymi w sieci, potencjalnie szkodliwe treści wygenerowane przez użytkowników oraz wykorzystywanie (nadużycia) informacji osobistych przez innych.

Najważniejsze wyniki zostały zawarte w opracowaniu „Risks and safety on the internet. The perspective of European children"[6]:

1. Powszechność dostępu i umiejętności internetowe dzieci

Internet jest mocno zakorzeniony w codziennym życiu dzieci: 93% europejskich 9-16-latków korzysta z niego co najmniej raz tygodniowo (60% codziennie lub prawie codziennie). Najczęściej dzieci korzystają z Internetu w domu (87%) i w szkole (63%). Lecz dostęp ulega większemu zróznicowaniu: 49% ma dostęp we własnym pokoju, a 33% w urządzeniach mobilnych (konsole do gier i smatfony).

Dzieci podejmują w sieci wiele potencjalnie korzystnych aktywności: 9-16-latki wykorzystują Internet przy odrabianiu prac domowych (85%), do grania w gry sieciowe (83%), do oglądania filmów i klipów wideo (76%), do kontaktowania się przy pomocy komunikatorów (62%). Rzadziej używają poczty mailowej (31%), wykorzystują kamery internetowe (31%), serwisy P2P (16%) i prowadzą blogi (11%).

59% 9-16-latków ma własny profil w serwisie społecznościowym, w tym: 26% 9-10-latków, 49% 11-12-latków, 73% 13-14-latków i 82% 15-16-latków. Serwisy społecznościowe są najbardziej popularne w Holandii (80%), na Litwie (76%) i Danii (75%). Polska jest powyżej średniej (71%), a Niemcy mają miejsce trzecie od końca (51%).

Wśród dziecięcych użytkowników serwisów społecznościowych publicznie dostępne profile ma 26% z nich. Najwięcej na Węgrzech (55%), w Polsce – 34%. 29% użytkowników serwisów społecznościowych ma co najmniej 100 kontaktów.

Częste korzystanie z Internetu powoduje, że **dzieci z reguły uważają, że przewyższają umiejętnościami internetowymi rodziców**. 36% dzieci ma co do tego pewność, dalsze 31% myśli że jest to raczej prawda. Tylko 33% dzieci uważa się za mniej biegłych niż rodzice.

[6] Livingstone, S., Haddon, L., Görzig, A., and Ólafsson, K. (2011). *Risks and safety on the internet: The perspective of European children*. Full Findings. LSE, London: EU Kids Online. [http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU Kids II (2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf], strona z wszystkimi materiałami na temat badania: [http://www.eukidsonline.net].

2. Ryzykowne zachowania i zagrożenia

Ryzykowne zachowania nie zawsze prowadzą do pojawienia się realnych zagrożeń. Dzieci były pytane o to, czy stykały się z wybranymi zagrożeniami, a następnie o to, czy wywołało to u nich niepokój:

2a. Pornografia

Pornografia jest zwykle przedstawiana jako najczęstsze ryzyko, jakie przynosi dzieciom Internet. Badania tego nie potwierdzają. Częściej dzieci są narażone na spotkania z kimś, kogo nigdy wcześniej nie poznały osobiście (poza siecią).

14% dzieci w wieku 9-16 lat w ostatnich 12 miesiącach widziało w sieci obrazy (zdjęcia, filmy itp.) „w oczywisty sposób związane z seksem – na przykład nagich ludzi, ludzi uprawiających seks". Spośród dzieci, które widziały obrazy związane seksem lub pornograficzne w sieci, jedno na troje było tym doświadczeniem zaniepokojone, a połowa (czyli jedno na sześcioro, które widziały obrazy związane z seksem lub około 2% wszystkich dzieci) poczuła się znacznie lub bardzo zaniepokojona tym, co zobaczyła.

Jednak te wyniki należy spojrzeć z szerzej perspektywy. Internet nie jest wyjątkowym źródłem tych doświadczeń. Z badań wynika, że 12% dzieci w ciągu ostatnich 12 miesięcy widziało treści związane z seksem lub pornograficzne za pośrednictwem telewizji i video. Tak więc **Internet w zasadzie podwaja ryzyko zagrożenia, ale nie stanowi w tym zakresie nowej jakości.**

Duże znaczenie ma to, jak dzieci reagują w przypadku zagrożenia. **53% dzieci, które zaniepokoiły się tym, że zobaczyły w sieci obrazy związane z seksem, powiedziało o tym komuś ostatnim razem, gdy to się wydarzyło**: 33% powiedziało o tym koledze, 25% – rodzicom. Jednak 25% dzieci po prostu przestało przez pewien czas korzystać z Internetu, a niektóre zmieniły ustawienia filtrów lub ustawienia dotyczące kontaktów. Warto zastanowić się, czy rzadkie zwracanie się do rodziców nie jest wynikiem niskiej oceny przez dzieci ich umiejętności internetowych? A może wynika z braku zaufania do dorosłych i pruderyjnego wciąż wychowania?

2b. Napastowanie (*bullying*)

Analizując rozmiary napastowania w sieci stwierdzono, że 6% dzieci w wieku 9-16 lat otrzymało przykre lub złośliwe wiadomości, a 3% samemu wysłało tego rodzaju wiadomości innym. Ponad połowa dzieci, które otrzymały napastliwe wiadomości była znacznie lub bardzo tym zaniepokojona.

Ponieważ 19% dzieci było napastowanych w sieci lub poza nią (w tym 6% w sieci) wydaje się, że **napastowanie częściej przydarza się dzieciom poza Internetem**.

Większość dzieci, które otrzymały przykre lub złośliwe wiadomości w sieci, zwróciło się po wsparcie. Tylko co czwarte dziecko nie powiedziało o zdarzeniu nikomu. 60% dzieci wykorzystało także dostępne w Internecie strategie radzenia sobie – usuwanie krzywdzących wiadomości albo blokowanie napastnika. Ten ostatni sposób dzieci postrzegają jako efektywny.

2c. Wiadomości o podtekście seksualnym (*seksting*)

15% dzieci w wieku 11-16 lat otrzymało w sieciach wymiany plików (peer to peer) „wiadomości lub obrazy związane z seksem… [co oznacza] wypowiedzi na temat uprawiania seksu lub obrazy nagich albo uprawiających seks ludzi", przy czym 3% przyznaje się, że wysłało lub opublikowało tego rodzaju przekazy.

Wśród dzieci, które otrzymały takie wiadomości, prawie jedna czwarta poczuła się zaniepokojona. Co więcej, spośród tych zaniepokojonych dzieci, prawie połowie zrobiło się znacznie lub bardzo nieprzyjemnie. Podsumowując, co ósme dziecko, które otrzymało przekazy związane z seksem (prawie 3% wszystkich dzieci), przejęło się tym znacznie lub bardzo.

Wśród dzieci, którym sprawiły przykrość wiadomości o podtekście seksualnym, 40% usunęła niechciane wiadomości związane z seksem lub zablokowała osobę (możliwość kontaktu z osobą), która je wysłała (38%). W większości przypadków dzieci potwierdzały, że takie działanie rozwiązało problem. Należy zachęcać więcej dzieci do stosowania tego rodzaju konstruktywnych sposobów radzenia sobie z zagrożeniami w sieci.

2d. Spotkania się osobiste z kimś poznanym w Internecie

Najpowszechniejszą ryzykowną aktywnością jest spotykanie kogoś, kogo wcześniej się nie znało. **30% dzieci komunikowało się w przeszłości z kimś, kogo nigdy wcześniej nie poznały osobiście (poza siecią**). Ten rodzaj aktywności może być ryzykowny, może też jednak być formą zabawy (rozrywki).

9% dzieci w ciągu ostatniego roku spotkało się poza siecią (osobiście) z kimś poznanym w Internecie. 1% wszystkich dzieci (lub jedno na siedmioro tych, które poszły na takie spotkanie) spotkanie tego rodzaju zaniepokoiło.

Jakkolwiek tego rodzaju spotkania poza siecią w najmniejszym stopniu dotyczą 9-10-latków, to jednak właśnie dzieci w tym wieku były najbardziej zaniepokojone tego rodzaju zdarzeniem (31% wśród tych, które poszły na spotkanie z osobą poznaną w sieci).

2e. Inne ryzykowne sytuacje

Drugim pod względem częstości występowania ryzykiem jest kontakt z potencjalnie szkodliwymi treściami publikowanymi przez użytkowników Internetu. **21% 11-16-latków było narażonych na jedno lub więcej rodzajów treści tego typu**. Były to treści związane z nienawiścią (12%), zachęcające do zachowań grożących anoreksją (10%), samookaleczeniem (7%), zażywaniem narkotyków (7%) i samobójstwem (5%).

9% dzieci w wieku 11-16 lat doświadczyło nadużycia ich prywatnych danych: wykorzystania hasła (7%) lub informacji osobistych (4%), a 1% zostało oszukanych finansowo w sieci.

30% dzieci w wieku 11-16 lat zgłasza, że na jeden lub więcej sposobów doświadczyło nadmiernego używania Internetu (np. zaniedbując przyjaciół, obowiązki szkolne, sen) – w „znacznym stopniu" lub „bardzo często".

3. Porównanie wyników z różnych krajów

Okazuje się, że przy łącznym rozpatrywaniu wszystkich zagrożeń dzieci z Europy w wieku 9-16 lat, które zetknęły się z co najmniej jednym z nich, stanowią mniejszość – odsetek tych dzieci wynosi 41%. Napotkanie przynajmniej jednego z zagrożeń w sieci dotyczy do 60% dzieci na Litwie, w Estonii, Republice Czeskiej i Szwecji. Najniższe wskaźniki doświadczania zagrożeń odnotowano w Portugalii, we Włoszech i w Turcji.

Natomiast **zaniepokojenie lub przykrość związaną z korzystaniem z Internetu deklaruje więcej dzieci z Danii (28%), Estonii (25%), Norwegii i Szwecji (23% w obu krajach), Rumunii (21%)**, a mniej dzieci z Włoch (6%), Portugalii (7%) i Niemiec (8%). W Polsce odsetek ten wynosi 11%.

Im więcej dzieci w danym kraju korzysta z Internetu codziennie, tym większy odsetek napotyka jedno i więcej zagrożeń. Jednakże częstsze korzystanie przynosi również więcej pozytywnych doświadczeń, możliwości oraz korzyści.

Najwięcej rodzajów aktywności podejmują w sieci właśnie dzieci z Litwy, Republiki Czeskiej, Estonii, Francji i Szwecji, a najmniej jej rodzajów podejmują dzieci z Irlandii i Turcji. Innymi słowy, **korzystanie z Internetu niesie ze sobą i zagrożenia, i możliwości. Niełatwo jest je dokładnie rozgraniczyć**.

4. Hipotezy co do przyczyn różnicowania sytuacji w poszczególnych krajach

Weryfikacji poddano wyjaśnienie wpływu zewnętrznych czynników na zróżnicowanie sytuacji między poszczególnymi krajami. Sprawdzano hipotezę, zgodnie z którą intensywność ryzykownych zagrożeń i reagowanie na to ryzyko zależy od: zamożności kraju (mierzonej wysokością PKB na głowę), regulacji prawnych odnoszących się do filtrowania/blokowania treści w Internecie i wolności prasy oraz dostępności technicznej Internetu, szczególnie szerokopasmowego.

Poziom ryzyka i bezpieczeństwo dzieci w sieci w małym stopniu statystycznie zależy od zamożności kraju (6,2% wariancji jest tłumaczony przez PKB). Dzieci w zamożnych krajach nordyckich często znajdowały się z ryzykownych sytuacjach. We Włoszech, Hiszpanii, Irlandii

i Wielkiej Brytanii wyższy PKB nie jest związany z wyższym poziomem ryzyka w sieci, a na Litwie, w Estonii i w Republice Czeskiej poziom ryzyka jest wysoki pomimo niskiego PKB.

Wyniki badań prowadzą również do ważnego wniosku, że **wymóg i częste stosowanie narzędzi filtrowania Internetu nie skutkuje statystycznie istotnym wpływem na poziom sieciowego ryzyka**. Choć okazuje się, że w części krajów w których często stosowane jest filtrowanie i blokowanie sieci, takich Wielka Brytania, Irlandia, Portugalia, jest także niższy poziom sieciowego ryzyka.

Poziom ryzyka w sieci jest negatywnie, choć w małym stopniu, powiązany z indeksem wolności prasy (4,4% wariancji jest tłumaczone przez indeks).

Rożne czynniki świadczące o powszechności dostępu do Internetu (czas jaki minął od kiedy 50% gospodarstw domowych jest dołączona do sieci, czas spędzany codziennie w sieci) nie mają wpływu na poziom ryzyka i bezpieczeństwo dzieci w sieci. **Z technicznych wskaźników tylko dostęp do szerokopasmowego Internetu w małym, choć istotnym, stopniu wpływa na poziom ryzyka w sieci** (6,2% wariancji jest tłumaczony przez dostęp do szerokopasmowego Internetu).

5. Wnioski

Kilkanaście (19) rekomendacji zostało ujęte w odrębnej publikacji „Final recommendations for policy, methodology and research”[7].

Rekomendacje podzielono na trzy grupy i odnoszą się one do: (1) użytkowników i ich aktywności sieciowej, (2) ryzykownych zachowań i zagrożeń oraz (3) wskazówek co do właściwych kierunków zaangażowania osób, które kształtują warunki, w jakich znajdują się dzieci. Sformułowano także wskazówki dla każdego z objętych badaniem państw.

Warto zatrzymać się na kilku rekomendacjach. Generalnie zalecają oni wyważone działania, czyli proporcjonalne do zagrożeń reagowanie oraz tworzenie zasobów i potencjału dla pozytywnego działania:

Zalecenie nr 1: **Na ile to możliwe, należy zachęcać dzieci do odpowiedzialności za własne bezpieczeństwo w sieci**. W przyszłości rodzice będą mieli jeszcze mniejsze niż obecnie możliwości wpływania na zachowania dzieci. **Dzieci mają prawo do ochrony i bezpieczeństwa, ale muszą ponosić odpowiedzialność za bezpieczeństwo i respektowanie praw innych**.

Zalecenie nr 17: **Aby techniki filtracji i oprogramowanie rodzicielskie do monitorowania dziecięcych zachowań uczynić bardziej akceptowalnymi, powinny one w większym stopniu uwzględniać potrzeby użytkowników**. Dla osiągnięcia skuteczności należy brać pod uwagę zainteresowania rodziców. Ich potrzeby nie ograniczają się do

[7] O'Neill, Brian and Livingstone, Sonia and Mclaughlin, Sharon (2011) *Final recommendations for policy, methodology and research*. EU Kids Online network, London, UK. [http://eprints.lse.ac.uk/39410/].

filtrowania treści związanych z seksem, bądź innych niewłaściwych dla dziecka treści, lecz odnoszą się też do monitoringu czasu spędzanego w sieci, czy blokowania przekazów o charakterze handlowym.

Zalecenie nr 18: Stopień zaangażowania nauczycieli jest wysoki, lecz powinien być podwyższony. Tylko poprzez szkoły można dotrzeć do wszystkich dzieci. **Zadaniem szkół powinno być docieranie do dzieci, do których z istoty "trudno docierać"**.

Zaleczenie nr 19: **Pośrednicy internetowi powinni być bardziej aktywni w promowaniu świadomości zagrożeń i w edukacji użytkowników**. Celem poprawy zaufania powinni umożliwiać i promować ustalane przez użytkowników właściwe dla dzieci opcje prywatności. Konfigurowanie tych funkcji powinno być przejrzyste. Powinna być stworzona możliwość fachowej niezależnej oceny tego oprogramowania.

Podstawowym celem powinno być ukształtowanie kompleksowej polityki uwzględniającej złożoność sytuacji, w jakiej znajdują się dzieci i wszyscy odpowiedzialni za ich wychowanie. **Celem tej polityki powinno być zachowanie w tak trudnych okolicznościach podmiotowości dzieci**. Jest to osiągalne przez podwyższanie umiejętności osób zaangażowanych w procesy wychowawcze, czyli głównie rodziców i nauczycieli.

Działania ze strony państwa, gospodarki, trzeciego sektora powinny służyć wspieraniu tak postawionych celów, a nie realizować cele autonomiczne, co niewątpliwie ma miejsce w przypadku programu „Bezpieczniejszy Internet" w obecnym kształcie. **Nie należy koncentrować się na „ściganiu zła"; trzeba rozwiązywać problemy wychowawcze**. W szczególności uwrażliwić na kwestię związaną z zachowywaniem niezbędnej kontroli i szybkości reakcji, łącznie z koniecznością przygotowania rodziców do roli pierwszej pomocy dla dzieci oraz wyczuleniem ich na obserwację symptomów, które mogą wskazywać na podejmowanie przez dzieci niebezpiecznych czy nielegalnych zachowań.

Bliższa analiza opracowań powstałych w ramach EU Kids Online II na tle dotychczasowych działań Programu „Bezpieczniejszy Internet" pozwoliłaby jeszcze wyraźniej niż powyżej wskazać jego ograniczenia i niedostosowania do realiów współczesnego społeczeństwa.

Józef Halbersztadt, Internet Society Poland

Jarosław Lipszyc, Fundacja Nowoczesna Polska

Katarzyna Szymielewicz, Fundacja Panoptykon

Jakub Śpiewak, Fundacja Kidprotect.pl

Michał Woźniak, Fundacja Wolnego i Otwartego Oprogramowania

Aleksander Waszkielewicz, Fundacja Instytut Rozwoju Regionalnego

Paweł Kaźmierczak, Fundacja Terebint