Katarzyna Badźmirowska – Masłowska

ROZWÓJ NOWYCH TECHNOLOGII KOMUNIKACYJNYCH A BEZPIECZEŃSTWO DZIECI W UNII EUROPEJSKIEJ (1996 – 2011). PERSPEKTYWA PRAWNA

Wstęp

Zmiany paradygmatu komunikowania, powstające w związku z pojawianiem się nowych technologii, determinują rozwój społeczeństw, dla których fundamentem staje się przepływ informacji. Wpływ środków masowego przekazu, a obecnie szerzej – środowiska nowych technologii komunikacyjnych, na rozwój dzieci i młodzieży nie budzi wątpliwości, choć jego zakres i stopień uwarunkowany jest wieloma, różnorodnymi czynnikami zarówno o charakterze endo, jak i egzogennym. Kluczową rolę w zachodzących procesach społecznych odgrywają klasyczne i nowe media, które niejako zastępują – tradycyjnie najistotniejsze dla kształtowania jednostki – oddziaływania rodziny, szkoły czy środowiska rówieśniczego. Szczególna rola przypada tu audiowizualnym środkom przekazu, przy czym należy zauważyć, że współcześnie różnorodne kategorie mogą być obejmowane tym pojęciem. Zasadniczo wyodrębnia się audiowizualne usługi medialne w rozumieniu dyrektywy 2010/13 oraz tzw. nowe media. W pierwszej grupie zawarte jest zarówno tradycyjne, linearne rozpowszechnianie telewizyjne, jak i nielinearne usługi 'na żądanie'; druga łączy się z usługami *on-line*, w ramach których następuje zarówno internetyzacja mediów masowych, jak i pojawianie się nowych form komunikacyjnych, charakteryzujących się zwłaszcza interakcyjnością, ale też możliwością ograniczania w różnym stopniu publiczności przekazu. Internet i inne nowe technologie oferują coraz to bardziej zróżnicowane, także jeśli chodzi o aspekty kulturowe, formy przekazu dla ich użytkowników/konsumentów, np. gry wideo, aplikacje hybrydowe, etc.[1]. Trzeba jednak pamiętać, że stanowią one niejako dodatkowe środki techniczne rozpowszechniania różnorodnej, także nielegalnej (prawem zakazanej), lub potencjalnie szkodliwej dla rozwoju małoletnich zawartości. Tak charakteryzowane środowisko kreuje specyficzne wyzwania w zakresie ochrony dzieci i młodzieży. Oczywiste zróżnico-

1) W ramach definicji nowych mediów uwzględnia się też niekiedy blogi, podcastingi, aplikacje hybrydowe, czy pocztę elektroniczną a nawet oprogramowania komputerowe; ponadto rozszerza się zakres urządzeń odbiorczych: DVD, palmtopy, tablety, PDA i odtwarzacze mp3, mp4. Kwestie terminologiczne wyjaśniające relacje między pojęciami komunikacji a komunikowania społecznego przekraczają ramy niniejszej pracy; tu są one stosowane zamiennie z innymi, tj. środowisko nowych technologii, *on-line*, etc.
por. np. 3. Cellary W. (red.), *Przemiany społeczne*, [w:] *Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym*, Wyd. UNDP, Warszawa 2002; K. Chałubińska–Jentkiewicz, *Media audiowizualne. Konflikt regulacyjny w dobie cyfryzacji*, Wolters Kluwer Polska, Warszawa 2011; Dijk, J. van, *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci.* Warszawa 2010; L. Gorman, D. McLean, *Media i społeczeństwo. Wprowadzenie historyczne*, WAiP, Kraków 2010, H. Jenkins, *Kultura konwergencji, zderzenie starych i nowych mediów*, WAiP, Warszawa 2007; R. Sierocki, M. Sokołowski, *Metafory sieci. (Re)definiowanie Internetu*, [w:] M. Jeziński (red.), *Nowe media w systemie komunikowania: Edukacja, cyfryzacja*, Wyd. A. Marszałek, Toruń 2011.

wanie globalnego obszaru audiowizualnego tworzy przesłanki dla nieco odmiennego regulowania medialnych usług audiowizualnych i innych usług *on-line*, w zależności od ich typu, przy zachowaniu jednak wspólnych dla całego sektora pryncypiów i standardów; chodzi tu bowiem o skuteczność realizacji zakładanych celów, co jest możliwe przy zastosowaniu odpowiednich dla danego środowiska metod i środków. Kwestia ta odnosi się także do kształtowania systemu ochrony dzieci i młodzieży przed negatywnymi dla nich treściami. W Unii Europejskiej rozróżnienie to widoczne było już w pierwszych dokumentach poświęconych tym zagadnieniom, w których proponowano nieco odmienne systemy rozwiązań dla masowych mediów audiowizualnych oraz rozwijających się innych usług *on-line*[2].

Unia Europejska wyznacza standardy odnośnie ochrony, obejmując swoją działalnością zasadniczo dzieci i młodzież do 18 roku życia. Odnotowania wymaga fakt, że w dyrektywach dotyczących audiowizualnego sektora medialnego posługuje się ona pojęciem małoletnich (*minors*), natomiast względem usług *on-line* raczej używany jest termin dzieci (*children*). Opierając się na uniwersalnym standardzie *Konwencji o prawach dziecka,* oznacza ono: *każdą istotę ludzką w wieku poniżej osiemnastu lat, chyba że zgodnie z prawem odnoszącym się do dziecka uzyska ono wcześniej pełnoletniość* (art. 1). Ogólnie zatem można w obydwu przypadkach zasadniczo mówić o osobach, które nie przekroczyły progu dorosłości, jednak z analizy dokumentów unijnych wynika, że jeśli chodzi o sektor nowych technologii, w większym stopniu zwraca się uwagę na najmłodsze kategorie wiekowe konsumentów/ użytkowników; wynika to prawdopodobnie z samego charakteru tego sektora, w którym kontrola rodzicielska/ opiekuńcza nastręcza większych trudności niż w przypadku audiowizualnych usług medialnych[3].

Zgodnie z art. 3 Konwencji państwa zobowiązane są dążyć do jak najlepszego zabezpieczenia interesów dziecka, w tym zapewnienia mu ochrony i opieki wymaganej dla jego dobra poprzez stworzenie i realizację właściwego systemu administracyjno – prawnego, jednocześnie *biorąc pod uwagę prawa i obowiązki jego rodziców, opiekunów prawnych lub innych osób prawnie za nie odpowiedzialnych*, czyniąc to poprzez podejmowanie wszelkich właściwych środków ustawodawczych i administracyjnych[4]. Podobnie, zgodnie z art. 24 *Karty Praw Podstawowych* UE, władze publiczne i instytucje prywatne mają przede wszystkim na uwadze dobro/ interes

2) Niniejsze opracowanie poświęcone jest zasadniczo dostępnym publicznie usługom elektronicznego środowiska *on-line*.
3) *Konwencja oprawach dziecka z 20 listopada 1989 roku,* Dz. U. z 1991 r. Nr 120, poz. 526.
4) Por. M. Sitek, *Prawne i instytucjonalne ramy zwalczania handlu ludźmi,*[w:] Sitek B., Dammacco G. i in. (red.), *Wykorzystywanie człowieka w XX i XXI wieku,* UWM Wydział Prawa i Administracji, Olsztyn 2012, s. 331-344

dziecka; małoletni zaś mają prawo do ochrony, koniecznej dla ich dobra, z uwzględnieniem ich wieku i stopnia dojrzałości ich poglądów[5].

Należy respektować prawa dzieci do wolności myśli, sumienia i wyznania oraz na podstawie tego standardu zagwarantować im prawo do swobodnej wypowiedzi: poszukiwania, otrzymywania i przekazywania idei i informacji, niezależnie od granic i form, w jakich się to odbywa. Ograniczenia są dopuszczalne, o ile są konieczne m.in. dla ochrony bezpieczeństwa społecznego, moralności publicznej, wyrażanej w państwach członkowskich w obszarze audiowizualnym poprzez samo-definiowanie interesu publicznego w ujęciu narodowym, którego istotną częścią jest ochrona dzieci i młodzieży; standard ten, co oczywiste, powinien dotyczyć także internetyzowanych mediów oraz innych usług *on-line* (art. 14 w zw. z art. 13 *Konwencji*). Celowe wydaje się tu odrzucenie skrajnych stanowisk zabraniających z jednej strony jakichkolwiek ograniczeń w środowisku Internetu, z drugiej zaś wprowadzających cenzurę i nadmierną kontrolę. Zrównoważenie obydwu tych podejść może mieć miejsce, jeśli za kryterium ewentualnego, przy zbalansowaniu z innymi prawami, wprowadzania restrykcji przyjąć ochronę małoletnich jako – wspólnej dla krajów członkowskich UE – przesłanki dla realizacji interesów narodowych w tym zakresie; zasada subsydiarności i proporcjonalności powinna być tu jednak stosowana na wszystkich poziomach, włącznie z krajowym. Analizując dokumenty unijne, można przyjąć, że tak się właśnie dzieje. Komisja Europejska precyzuje bowiem: *Przeciwdziałanie zagrożeniom i wzmacnianie bezpieczeństwa w społeczeństwie cyfrowym to wspólna odpowiedzialność osób prywatnych i organów publicznych, na szczeblu lokalnym i globalnym. W celu zwalczania wykorzystywania seksualnego i rozpowszechniania materiałów związanych z seksualnym wykorzystywaniem dzieci w Internecie, na szczeblu krajowym i unijnym ustanowić można platformy ostrzegania, jak również stosować środki zezwalające na usuwanie szkodliwych treści i zapobieganie ich wyświetlania. Niezbędne jest również prowadzenie działań edukacyjnych i kampanii informacyjnych dla ogółu społeczeństwa (...). Należy również zachęcić przedstawicieli przemysłu do opracowania i wdrożenia systemów samoregulacji, w szczególności w odniesieniu do ochrony nieletnich korzystających z ich usług.* Rada natomiast konkluduje*: Ważne jest, by państwa członkowskie, Komisja, przemysł audiowizualny i dostawcy usług internetowych byli świadomi nowych wyzwań w zakresie wzmocnienia pozycji i ochrony małoletnich, które to wyzwania*

5*) Karta praw Podstawowych*, OJ. 14.12.2007, C 303; por. Wyrozumska A., *Znaczenie prawne zmiany statusu Karty Praw Podstawowych Unii Europejskiej w Traktacie Lizbońskim oraz Protokołu Polsko-Brytyjskiego*, Przegląd Sejmowy 2008 Nr 2(85), str. 25–39. Osobnego opracowania wymagają kwestie niegodziwego traktowania i seksualnego wykorzystywania dzieci, por. np. M. Gruchoła, *Ochrona małoletnich internautów w prawie i praktyce Unii Europejskiej,* Rozprawy Społeczne, nr 1 (V) 2011, s. 78 – 89.

wynikają z rozwoju w dziedzinie audiowizualnych i internetowych usług informacyjnych, ale też by zdawali sobie sprawę z istnienia instrumentów mających służyć reagowaniu na te wyzwania[6].

Powyższe sformułowania świadczą o tym, że instytucje UE przywiązują dużą wagę do omawianych zagadnień. Stanowią one jednocześnie pewnego rodzaju ramy, standardy, w których operować powinny państwa członkowskie, a szerzej wszystkie zainteresowane strony reprezentujące zarówno przemysły nowych technologii, jak i środowiska organizacji pozarządowych czy wreszcie samych rodziców, opiekunów, nauczycieli czy małoletnich; co istotne, działają one w ścisłej współpracy zwłaszcza z Komisją Europejską i pod auspicjami UE. Mimo iż finalnymi adresatami działań są dzieci i młodzież oraz najbliższe im środowiska rodzinne i szkolne, efektywność przyjmowanych rozwiązań w warunkach transgraniczności omawianego obszaru musi opierać się o kooperację ponad i międzynarodową i podlegać koordynacji na poziomie unijnym. Można zauważyć, że Unia reaguje na zmieniające się środowisko audiowizualne, dostrzegając pojawiające się coraz to nowe wyzwania i próbując stosować adekwatne metody i środki ukierunkowane na skuteczną ochronę małoletnich; w tym celu dokonuje odpowiednich zmian w ramach już stosowanych narzędzi, wprowadza nowe, kompilując je w spójne systemy przeznaczane dla danego typu usług. Sektor treści audiowizualnych postrzegany jest szeroko, obejmując zagadnienia łączące się np. ze specyfiką ich udostępniania w nowych warunkach (gry wideo *on-line*) czy tworzenia się nowych lub modyfikacji istniejących już form w związku np. z rozwojem technologii mobilnymch.

Poszerzający się zakres oferowanych treści i ich form skutkuje coraz większymi problemami w zakresie ochrony dzieci i młodzieży. Prześledzenie poszczególnych etapów działalności UE w kontekście stosowania miękkich i twardych środków prawnych w powyższym zakresie wydaje się ważne z punktu widzenia projektowania adekwatnych dla współczesnych wyzwań systemowych rozwiązań. Zwłaszcza jeśli chodzi o nowe, narastające zagrożenia, do których dochodzi poprzez systemy teleinformatyczne lub sieci telekomunikacyjne, tj. uwodzenie dzieci (*grooming*) czy nękanie, ośmieszanie, wyzywanie, kompromitowanie, szantażowanie (*cyber-bullying*)[7].

Etapy i kierunki rozwoju środowiska nowych technologii komunikacyjnych znajdują odzwierciedlenie w rozwiązaniach proponowanych dla zagwarantowania efektywnej ochrony małoletnich, zawartych w ko-

6) *Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions a digital agenda for Europe* COM (2010) 245 final/2; European Parliament resolution of 5 May 2010 *on a new Digital Agenda for Europe*: 2015.eu (2009/2225(INI)); *Council conclusions* of 31 May 2010 *on digital agenda in Europe*, COM/2010/0245 final.

7) Por. art. 200a *kodeksu karnego 6 czerwca 1997 r.,* Dz. U. 1997nr 88 poz. 533 z późniejszymi zmianami, kodeks-karny.org (19.06.2012).

lejnych, posiadających różnorodny charakter, dokumentach Unii Europejskiej; niekiedy nadaje się im charakter prawnie wiążący, pod warunkiem jednakże zastosowania zasady subsydiarności. Chronologicznie, poczynając zasadniczo od zielonej księgi z 16.10.1996 roku *o ochronie małoletnich i godności ludzkiej w audiowizualnych i informacyjnych usługach*[8], poprzez m.in. programy bezpieczniejszego Internetu (1999 – 2013), aż do odnośnej strategii z 2012 roku[9], UE dąży do obejmowania swoimi działaniami całokształtu zagadnień. Dlatego wraz ze zmianami cywilizacyjnymi wzrasta liczba dokumentów i obejmowany nimi obszar problemowy. Przyjmuje się lub korzysta z ogólnych standardów konwencyjnych, Karty Praw Podstawowych, dyrektyw, etc., uzupełniając je rekomendacjami, komunikatami, rezolucjami, studiami, programami czy wreszcie strategią. Szeroki wachlarz stosowanych instrumentów zawiera różnorodne metody, środki i narzędzia, tj. 1) samo i ko-regulacje, kodeksy dobrych praktyk, 2) zabezpieczenia techniczne i systemy oznakowań/ oznaczeń zawartości (w formie kategoryzacji wiekowych lub klasyfikacji treści[10]), 3) edukacja do szeroko rozumianego środowiska nowych technologii; podkreśla się znaczenie ustalania standardów na poziomie nie tylko krajowym, ale przede wszystkim na unijnym czy międzynarodowym. Mimo że – jak już o tym była mowa – finalnymi ich adresatami są małoletni i ich środowiska rodzinne (w pewnym stopniu także szkolne), to obowiązki prowadzenia określonych działań nakłada się zarówno na UE (głównie Komisję Europejską), państwa członkowskie, przedstawicieli odpowiednich przemysłów, czy wreszcie innych zainteresowanych stron (np. organizacji pozarządowych); współpraca ponadnarodowa i między sektorami publicznym i prywatnym jest bowiem podstawą do tworzenia i możliwie najskuteczniejszego i systemowego realizowania celów i zadań wynikających z ochrony małoletnich w nowym środowisku usług komunikacyjnych. Żadne jednak środki nie są wystarczająco efektywne i nie mogą zastąpić kontroli rodzicielskiej, dlatego szeroko rozumiane zagadnienia edukowania społeczeństwa (zwłaszcza użytkowników końcowych) nabierają szczególnego znaczenia; ważne znaczenie mają więc kwestie praktycznych umiejętności w korzystaniu z narzędzi kontroli rodzicielskiej. Dlatego szczególny nacisk położono na kwestie związane z sytuacją rodziców/ opiekunów jako osób bezpośrednio odpowiedzialnych za skuteczność prowadzonych polityk; temu zagadnieniu poświęcony jest ostatni punkt opracowania.

8) COM (96) 483 final.
9) Zagadnienie europejskiej strategii w kierunku bezpieczniejszego internetu dla dzieci, wymaga odrębnego opracowania, *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European strategy for a better internet for children,* COM (2012) 196 final.
10) Szerzej por. pkt 5, przypis 51.

1. Geneza ochrony małoletnich w UE w sferze usług on – line

Już w zielonej księdze z 16.10.1996 roku *o ochronie małoletnich i godności ludzkiej w sferze usług audiowizualnych i informacyjnych*[11] wskazano, że ochrona dzieci i młodzieży w związku z rozwojem nowych technologii staje się coraz bardziej złożona; dostosowujący się do jego poziomu przemysł zaczął więc wprowadzać szereg nowych – względem stosowanych w sektorze mediów audiowizualnych – mechanizmów dla dostawców treści, warunkowego dostępu czy konsumentów/użytkowników. Co istotne, uznano, że tylko kompleksowy system umożliwi rodzicom/opiekunom sprawowanie efektywnej kontroli dostępu małoletnim do usług internetowych lub innych świadczonych drogą *on-line*. Wskazano na potrzeby: 1) dokonywania uprzedniej identyfikacji użytkowników, 2) umożliwiania rodzicom ograniczania czasu dostępu do w/w usług, 3) kontrolowania przez nich historii aktywności dzieci, 4) filtrowania materiałów pod kątem automatycznego relegowania zawartości nielegalnej (*illegal)* lub oznakowywania treści szkodliwych (*harmful).*

Kluczowym problemem usług *on-line* stała się kwestia klasyfikacji ich zawartości; ma to znaczenie, zwłaszcza jeśli uwzględni się fakt, że każdy użytkownik jest potencjalnie także jej dostawcą. W tym kontekście postulowano rozwijanie trzech typów filtrowania, obejmujących: 1) 'czarną listę' (*black list*) – ukierunkowaną na blokowanie dostępu do stron zidentyfikowanych jako problematyczne (np. zawierających sceny nagości, seksu, przemocy, etc.); uznano jednak, że listę tę trudno jest aktualizować; 2)' białą listę' *(white list)* – opartą o indywidualne, uprzednie określenie stron, do których dostęp jest uprawniony; wskazano tu na trudności w wyznaczaniu jej granic; 3) 'neutralną listę' (*neutrallabeIling)* – skonstruowaną na potrzeby użytkowników przez dostawców lub inne podmioty na podstawie przyjętych przez nich kryteriów. Zastosowanie kombinacji powyższych form klasyfikowania treści miało na celu umożliwienie rodzicom/ opiekunom stworzenia warunków stosunkowo bezpiecznego dostępu do Internetu przez dzieci i młodzieży; choć – jak podkreślono – tylko wprowadzenie generalnego systemu neutralnego oznakowania pozwoli na całościowe uregulowanie omawianej problematyki.

Rekomendacja Komisji (98/560/EC)[12], dotycząca środowiska usług in-

11*) Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services***,** COM (96) 483 final, 16 October 1996.

12) *Council Recommendation* 98/560/EC of 24 September 1998 *on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity* , O. J. L 270 of 7.10.1998; u podstaw powyższych rozwiązań stała wspólna rezolucja Rady i przedstawicieli rządów państw członkowskich. *Resolution of the council and*

formacyjnych i audiowizualnych i stanowiąca wytyczne dla krajowych legislacji, objęła wszystkie elektroniczne media. Z globalnej natury sieci komunikacyjnych, wynikła konieczność przyjęcia międzynarodowego do nich podejścia; transgraniczność usług audiowizualnych wymogła też wzmocnienie środków na poziomie unijnym, jako efektywniej realizujących zadania w tym sektorze. Istotnym elementem było tu ustanowienie narodowych ram, ukierunkowanych na lepsze rozumienie i stosowanie standardów europejskich i istniejących w ich ramach krajowych regulacji, dla przygotowywanych przez operatorów i dostawców usług *on-line*, samoregulacji i kodeksów dobrych praktyk; zainteresowane strony miały wypracowywać rozwiązania zgodnie z tradycjami narodowymi, we współpracy z właściwymi władzami i z uwzględnieniem kooperacji na poziomie europejskim.

Szczególnego znaczenia w tych warunkach nabrała kwestia rozgraniczenia treści nielegalnych, od prawem dozwolonej zawartości, nieodpowiedniej jednak dla osób małoletnich, z racji zagrożeń, jakie niesie ona dla prawidłowego psychicznego, fizycznego i moralnego ich rozwoju oraz stosowania względem nich odmiennych rozwiązań ochronnych.

Zgodnie z postanowieniami aneksu I, dedykowanego problematyce dostępnej publicznie zawartości usług *on-line*, zaakceptowano fakt, że tworzenie systemów samoregulacyjnych będzie się odbywało z poszanowaniem różnic w podejściu i wrażliwości charakterystycznej dla rozumienia interesu publicznego w ujęciu narodowym; według zawartych w nim wytycznych:

1. Zdefiniowanie, wdrażanie i ocena narodowych systemów samoregulacyjnych opiera się na pełnym udziale wszystkich zainteresowanych na poziomie krajowym stron, tj. władze publiczne, użytkownicy/ konsumenci, czy wreszcie – odpowiedzialne za system publiczne i prywatne podmioty gospodarcze, bezpośrednio lub pośrednio zaangażowane w przemysł usług audiowizualnych i *on-line*. Ich szeroki udział jest odzwierciedleniem podstawowej zasady – dobrowolności, która determinuje efektywność zarówno przyjętych, konkretnych zobowiązań, jak i wypełniania długoterminowych zadań, związanych z rozwojem wspólnych idei i narzędzi, tj. oznakowanie treści, kategoryzacje wiekowe, czy uzupełniających je sposobów informacji, uświadamiania i edukacji. Regularna ocena skuteczności krajowych systemów odbywać się miała w ramach interesu ogólnego, mierzącego poziom realizacji zakładanych celów i adaptowania ich do sukcesywnie zmieniających się warunków rynkowych i technologicznych;

2. Tworzenie, w ramach powyżej wskazanych systemów i na podstawie ich zasad kodeksów dobrych praktyk, czerpiących ze standardów samoregulacyjnych, ukierunkowanych na to, by małoletni bez zgody opiekunów nie mieli dostępu do treści legalnych, jednakże szkodliwych dla ich

of the representatives of the governments of the member states, meeting within the council of 17 february 1997 on illegal and harmful content on the internet, 97/C 70/01.

rozwoju. Podkreślono, że uwzględnione musi być zróżnicowanie (także w zakresie odpowiedzialności): a) przedmiotowe (usług) i b) podmiotowe (co do operatorów sieci, dostępu, zawartości, etc.) oraz c) wynikające ze środowiska nowych technologii (sieci zamknięte i otwarte, aplikacje o różnym poziomie interaktywności).

Szczególny nacisk położono na poprawienie stanu edukacji, w tym świadomości zagrożeń współczesnego środowiska usług on-line, poprzez: a) informowanie użytkowników o każdym ryzyku związanym z zawartością i dostępnych środkach przeciwdziałania, w tym powiadamianie o wyposażeniu technicznym, umowach z użytkownikami, etc., 2) wprowadzanie odrębnych reguł prezentacji treści potencjalnie szkodliwych dla rozwoju małoletnich, obejmujących informowanie o w/w charakterze zawartości, systemy ostrzeżeń (pisemne, dźwiękowe lub audiowizualne), opisowe lub klasyfikacyjne oznakowanie treści, lub weryfikujące wiek użytkownika; za priorytetowe uznano treści, tj. pornografia czy przemoc.

Za zasadne uznano wspieranie kontroli rodzicielskiej – poprzez dostarczanie łatwych w obsłudze narzędzi, pozwalających bez uprzedniego uczenia się na decydowanie przez nich o dostępie małoletnich do usług, nawet jeśli nie są one nadzorowane. Ułatwienia dla takiej kontroli powinny obejmować: oprogramowanie filtrujące, obsługiwane przez użytkownika i aktywowane na jego żądanie przez operatora usług, np. poprzez ograniczanie dostępu w ogólności lub do wcześniej definiowanych stron.

Wnoszenie skarg na zawartość niezgodną z zasadami ochrony małoletnich powinno się odbywać w ramach zorganizowanego efektywnego systemu tzw. gorących linii (*hot lines*), ułatwiających ich wysyłanie i odbiór poprzez np. telefon, email oraz procedurę rozpatrywania (z właściwą wymianą informacji między dostawcami usług lub treści, operatorami, etc.);

3. Ułatwianie przez państwa członkowskie na poziomie wspólnotowym współpracy krajowych struktur i wszystkich zainteresowanych stron, działających w systemach w/w skarg, w tym utworzenie tzw. krajowego punktu kontaktowego w celu zwalczania nielegalnej zawartości, wymianę doświadczeń i usprawnianie zgodnego z prawem i odpowiedzialnego korzystania z sieci[13].

W tym miejscu należy dodać, że rozwinięciem powyższych zaleceń była rekomendacja z 20. 12. 2006 roku[14], opierająca się m.in. o zapisy

13) Por. np. *Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 on protection of minors and human dignity,* COM(2001) 106final - 27.02.2001; *Second evaluation report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity"*, COM/2003/0776 final.

14) *This Recommendation covers new technological developments and complements Recommendation 98/560/EC. Its scope, on account of technological advances, includes audiovisual and on-line information services made available to the public via fixed or mobile*

art. 24 Karty Praw Podstawowych. Podkreślono w niej, że ochrona dzieci i młodzieży w środowisku usług informacyjnych, przed dostępem do treści przeznaczonych wyłącznie dla osób dorosłych, wymaga przyjęcia na poziomie UE środków prawnych; winna być ona rozpatrywana w ramach ochrony interesu obywateli Wspólnoty, utożsamianego tu z wolnością przepływu informacji, przy czym uwzględnić należy zapewnienie legalności zawartości oraz poszanowanie dla ludzkiej godności.

Zmieniający się krajobraz medialny, determinowany rozwojem nowych technologii wymagał szerokiej edukacji w zakresie efektywnego korzystania z informacyjnych usług *on-line*, jako elementu szerszego systemu uzupełnianego, na poziomie krajowym i europejskim, współpracą w ramach samo- i koregulacji, z władzami, przemysłem i społeczeństwem obywatelskim. Komisja zachęcała także powyższe podmioty do kooperacji w zakresie tworzenia klasyfikacji treści, kategoryzacji wiekowych w kontekście umożliwienia użytkownikom, w szczególności rodzicom i nauczycielom, raportowania nielegalnej zawartości i oceny dostępu do niej, podobnie jak i do, zgodnych z prawem treści, zagrażających lub mogących zagrażać rozwojowi małoletnich.

Kraje członkowskie zobowiązane zostały do promowania działań pozwalających na odpowiedzialne korzystanie zwłaszcza z usług internetowych, głównie poprzez poprawę stanu świadomości środowiska rodzinnego i szkolnego w zakresie potencjału tych usług i środków uczynienia ich bezpiecznymi dla dzieci i młodzieży; postulowaną formułą stało się nauczanie w ramach programów szkolnych. Dla przykładu w aneksie II wskazano na następujące działania państw, oparte o zintegrowane podejście do problematyki nauczania współczesnego środowiska nowych usług informacyjnych: 1) kontynuacja szkoleń nauczycieli i trenerów, we współpracy z organizacjami zajmującymi się ochroną dzieci, na temat ryzyka, jakie wiąże się z korzystaniem z niego, zwłaszcza jeśli chodzi o tzw. 'chatrooms' czy fora; 2) wprowadzenie szkoleń dla dzieci, także tych najmłodszych, z uwzględnieniem otwartych dla rodziców sesji; 3) dystrybucja pakietów informacyjnych o bezpiecznym korzystaniu z Internetu oraz ustanawianiu i usprawnianiu funkcjonowania tzw. gorących linii; 4) organizowanie krajowych kampanii medialnych i informacyjnych w omawianym wyżej zakresie.

Oczekiwano, że przedstawiciele przemysłu audiowizualnego i usług informacyjnych *on-line* i inne zainteresowane podmioty, także w drodze współpracy z regulatorami, ciałami samoregulacyjnymi i koregulującymi, będą rozwijać inicjatywy ułatwiające małoletnim szerszy dostęp do nowych technologii; skuteczne ograniczanie dostępu do potencjalnie

electronic networks (19); Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, O.J. L 378, 27.12.2006.

szkodliwej zawartości może zostać osiągnięte przez użycie systemów filtrujących, wspólnych opisowych symboli lub ostrzeżeń kategoryzujących według kryterium wieku lub klasyfikujących treści w usługach informacyjnych *on-line*. W aneksie III wskazano na przykładowe inicjatywy w tym zakresie: 1) systematyczne dostarczanie użytkownikom skutecznych, aktualnych i łatwych w obsłudze systemów filtrowania w ramach subskrybowanej oferty; 2) oferowanie dostępu do usług skierowanych do dzieci, wraz z wyposażeniem, posiadającym system automatycznego filtrowania obsługiwanym przez dostawców dostępu lub operatorów telefonii mobilnej; 3) wprowadzanie systematycznie aktualizowanych opisów dostępnych stron, ułatwiających ich klasyfikowanie i ocenę zawartości, co łączy się z rozwijaniem używania systemów oznaczania materiałów dystrybuowanych w Internecie; 4) szerokie propagowanie informacji o bezpieczeństwie w Internecie, w tym o działaniach tzw. gorących linii[15].

Komisja Europejska otrzymała zadania: 1) promowania i rozwijania programów bezpiecznego Internetu[16]; 2) zbadania możliwości wprowadzenia europejskiego, darmowego numeru telefonu (typu *hot line)* lub poszerzenia dostępności użytkowników do źródeł informacji, mechanizmu i procedur skarg, etc.; 3) rozpoznania możliwości rozszerzenia na poziomie unijnym monitorowania stron pod kątem poszanowania małoletnich i ich praw (tj. domena KID.eu); 4) wspierania inicjatyw tworzenia i rozwijania sieci ciał samoregulacyjnych, powołanych dla wymiany doświadczeń i dokonania oceny efektywności kodeksów postępowania i podejść opartych o systemy samoregulacyjne, pod kątem osiągania możliwie najwyższych standardów ochrony małoletnich; szczególne znaczeniema tu dialog między organizacjami skupiającymi dostawców treści, czy – z drugiej strony – konsumentów.

Po 2000 roku państwa członkowskie i KE zostały zobowiązane do intensyfikowania współpracy w powyższym zakresie, obejmując nią także szerszy asortyment produktów, tj. film, DVD czy video kasety; oznaczało to *de facto* rozszerzenie zakresu ochrony o nowe pola eksploatacyjne.

15) Inne zadania wyznaczono dla specjalistów, pośredników i użytkowników nowych technologii komunikacyjnych. Podkreślono potrzebę zachowania czujności i informowania o stronach uznanych za nielegalne, np. poprzez udział w kreowaniu kodeksów dobrych praktyk, tworzących, odpowiednie, co do jakościowego poziomu, standardy dla dostawców usług odpowiedni jakościowo poziom, co ułatwia użytkownikom rozeznanie w dostępnej ofercie.
16) Szerzej por. pkt 4.

2. Rozwój technologii jako determinant rozszerzania zakresu ochrony

Kwestię gier wideo wprowadzono do zakresu problematyki ochrony małoletnich już na początku XX wieku. W dniu 01. 03. 2002 r. Rada wydała rezolucję poświęconą ochronie konsumentów, zwłaszcza młodych ludzi poprzez oznakowywanie gier komputerowych i video zgodnie z kategoryzacją wiekową[17]; w praktyce oznaczało to objęcie ich regulacjami właściwymi dla nowego środowiska usług informacyjnych. Wynikało to z faktu rozwijania się rynku tych gier i szerokiej ich dostępności. Znaczne ich zróżnicowanie, także co do zawartości, kierunkowało je do różnych konsumenckich grup wiekowych; niektóre z nich nie są odpowiednie dla osób małoletnich z uwagi na szkody, jakie mogą wyrządzić w ich prawidłowym rozwoju. Podkreślając wagę dostępu konsumentów do pełnych informacji o charakterze zawartości, przyjęto, że proste, jasne do oceny systemy oznakowań stanowią istotny i przejrzysty sposób realizacji tego zadania na poziomie krajowym. Przyjmując kategoryzacje wiekowe, państwa członkowskie różnią się jednak między sobą, co jest wynikiem odmiennych wzorców kulturowych, indywidualnej wrażliwości – tego, co w istocie składa się na pojęcie interesu publicznego w ujęciu narodowym[18]; efektywność wymagała więc szerokiej współpracy zainteresowanych stron zarówno na poziomie krajowym, jak i wspólnotowym; za środek wspomagający uznano samoregulacje.

W komunikacie *on protection of consumers, in particular minors, in respect of the use of video games* z 28. 04. 2008 roku[19] , nawiązującym do odnośnej rezolucji Rady z 2002 roku, wskazano na potrzebę prowadzenia, przyjętego przez wszystkie zainteresowane strony, klarownego systemu oznaczania gier komputerowych i wideo *on-line*, z zastosowaniem kryterium wiekowego; szczególnego znaczenia w tym kontekście nabrało dokonywanie ocen zawartości, z uwzględnieniem przeglądu różnorodnych ich metod. Gry, stanowiąc zjawisko międzygeneracyjne, są ulubionymi rozrywkami nie tylko europejskich dzieci i młodzieży; grają w nie bowiem również rodzice z dziećmi czy sami dorośli. Niewątpliwie rozwijają one pozytywne umiejętności, tj. myślenie analityczne, strategiczne czy

17) *Council Resolution, of 1 March 2002 on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group* OJ. EC, C65, 14.3.2002, p.2.

18) Por. K. Chałubińska – Jentkiewicz, *Media audiowizualne..., dz.cyt.*, zwłaszcza rozdział 2 pkt 2.

19) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on the protection of consumers, in particular minors, in respect of the use of video games - 22 April 2008*, COM(2008) 207 final; por. też: *Report* of 16 February 2009, of *European Parliament on the protection of consumers, in particular minors, in respect of the use of video games*, 2008/2173(INI), Committee on the Internal Market and Consumer Protection.

obeznanie z nowymi technologiami[20]. Jednak bezpieczeństwo, zwłaszcza najmłodszych małoletnich jest zagrożone ze względu na znaczny, często negatywny wpływ omawianych gier na ich rozwój psychiczny i społeczny; zakres ochrony dzieci i młodzieży rozszerza się zatem o nowe, istotne pola. Kwestia ograniczania dostępu według kategorii wiekowych, w tym do treści przeznaczonych wyłącznie dla osób dorosłych, opiera się na systemie PEGI[21]; podniesiono kwestię wzrostu technologicznej i społecznej presji na ujednolicanie przyjmowanych przez państwa członkowskie klasyfikacji treści niezależnie od rodzaju usług audiowizualnych, w oparciu o przyjęcie wspólnych kryteriów, wypracowanych w drodze regularnej wymiany dobrych praktyk pomiędzy różnymi platformami medialnymi. Podkreślono też rolę edukacji medialnej ukierunkowanej na kształtowanie umiejętności technicznych (zdolności dostępu), rozumienia, oceny i tworzenia medialnej zawartości we wszystkich typach mediów, włączając w to także sektor gier wideo.

Zwiększająca się liczba gier wideo zawierających obrazy przemocy wymaga ograniczania ich dostępności w handlu detalicznym, dystrybucji i obrocie. Nie wszystkie państwa członkowskie dysponują szczególnymi uregulowaniami w tym zakresie, przy ocenie zawartości takich gier, biorąc pod uwagę regulacje np. prawa karnego czy cywilnego; niektóre kraje przewidują zakazy rozpowszechniania szczególnie brutalnych gier wideo, choć w opinii KE powinny one mieć charakter wyjątku i podlegać zasadzie proporcjonalności; preferuje się inne metody, tj. np. uzależnienie sprzedaży od zgody rodziców. Uzupełniająco stosuje się także instrumenty samo- i koregulacyjne, w których zasadniczym kryterium kategoryzującym jest wiek użytkownika. Analogiczna sytuacja występuje w przypadku

20) Szerokie ich rozpowszechnienie przyczynia się także do wzmacniania europejskiego przemysłu interaktywnych gier z użyciem szerokopasmowych sieci telekomunikacyjnych i trzeciej generacji telefonów komórkowych. Pojawiającym się nowym trendem staje sie dostarczanie popularnych gier wideo w darmowej wersji *on-line*, co rozszerza znacząco do nich dostęp; są one opatrywane reklamami.

21) W kwietniu 2003 roku przyjęto europejską samoregulację *Pan European Games Information age rating system* (PEGI), powstałą w wyniku ścisłej współpracy przemysłu i społeczeństwa obywatelskiego, reprezentowanego m.in. przez stowarzyszenia konsumenckie i rodzicielskie i opartą na kategoryzacjach wiekowych; PEGI *On-line* został ustanowiony w czerwcu 2007 roku jako odpowiednik systemu macierzystego w warunkach środowiska *on-line*, wspomagający rodziców w zakresie uświadamiania ryzyka i potencjalnej szkodliwości danych treści, http://www.pegi.info/en/index/id/33, http://www.pegionline.eu/pl/index (19.06.2012).

Por. też: ICRA (FOSI*)* system, administrowany przez *Family Online Safety Institute* jest inicjatywą samoregulacją, opartą o opisowe oznakowanie treści *on-line*, według charakteru zawartości, tj. nagość, seks czy wulgarny język oraz hazard, narkotyki czy alkohol, z uwzględnieniem grup wiekowych użytkowników; proponuje się zastosowanie odpowiednich systemów filtrujących., http://www.fosi.org/icra (19.06.2012); por. też *Quatro+ Project QUATRO Plus* http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2006-UE-211001 (20.06.2012).

gier *on-line*, przy czym tu niekiedy wyodrębnia się unormowania dotyczące dostępności internetowych gier komputerowych; zobowiązuje się też dostawców treści do informowania użytkowników o możliwościach instalowania filtrów zawartości. Komisja, pozytywnie oceniając dotychczasowe osiągnięcia państw członkowskich, zwłaszcza w stosowaniu systemu PEGI i PEGI *on-line,* uważa, że niezbędne są dalsze wysiłki w kierunku większego uwzględnienia specyfiki tego typu gier. Potrzebny jest szybki i skuteczny mechanizm weryfikacji wieku, wypracowany w ramach pan – europejskiego dialogu między wszystkimi zainteresowanymi stronami, w tym we współpracy publiczno – prywatnej, ukierunkowanej na zwalczanie w pierwszym rzędzie cyberprzestępczości, co za tym idzie nielegalnej lub potencjalnie szkodliwej dla małoletnich treści internetowej (w szczególności odnosi się to do tzw. *chat rooms* związanych z omawianymi tu grami*)*. Podobnie wspólny standard wydaje się konieczny, jeśli chodzi o dobre praktyki w zakresie sprzedaży gier dzieciom i młodzieży i zwiększania świadomości ich rodziców i opiekunów. Mimo sceptycyzmu niektórych państw członkowskich (w tym Polski) zachęca się je, w kooperacji ze wszystkimi zainteresowanymi stronami krajowymi, do podejmowania, pod auspicjami UE, wspólnych inicjatyw w zakresie tworzenia miękkich środków regulacyjnych, technicznych zabezpieczeń, klasyfikacji oznakowań treści, kategoryzacji wiekowej (w ramach systemów PEGI) oraz edukacji do środowiska nowych technologii.

Dynamiczny rozwój usług komunikacyjnych spowodował powstanie nowych inicjatyw w środowisku dostawców technologii lub zawartości, wykorzystywanych przez urządzenia mobilne (*mobile provider* – dalej MP), ukierunkowanych na uczynienie go bardziej bezpiecznym dla dzieci i młodzieży. Doprowadziło to do podpisania na poziomie UE w dniu 26.02.2007 roku porozumienia w sprawie ochrony małoletnich korzystających z urządzeń telefonii mobilnej[22]. Przyjęcie unijnych ram odzwierciedla potrzebę

22) Problematyka wzajemnych relacji między pojęciami 'mobile provider'(czy 'mobile operator') i 'content provider' przekracza ramy niniejszego opracowania; w momencie podpisywania porozumienia chodziło głównie o telefony komórkowe; obecnie pojęcie to ma szerszy zakres, obejmując m.in. iphony, ipady, etc.; *European Framework for Safer Mobile Use by Younger Teenagers and Children* SIPMC 07 2; *This framework is a self-regulatory approach to the classification and rating of commercial content on mobile phones and is designed to operate on an cross-media basis in each national market of the 27 Member States of the European Union* (…) *Rating under this Framework is done by commercial content providers, and mobile operators present in individual national markets – based on an agreed cross media classification scheme;* za: http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm; http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/Safer_Mobile_Flyer-1.pdf [dostęp: 26.06.2012]; por. też np. G. Goggin, *Cell Phone Culture: Mobile Technology in Everyday Life*, Londyn 2006.
Także *The Safer Internet Programme* koncentruje się na tej kwestii od 2005 roku, od czasu przeprowadzonej w ramach *Safer Internet Forum* debaty*;* w lipcu 2006 r. rozpoczęły się publiczne konsultacje w tej materii*;* Online technologies for children (2007); Child safety and mobile phone services (2006).

wspierania bezpieczeństwa w obszarze nowopowstających technologii. Usługi mobilne w istocie oferują konsumentowi dodatkowy kanał/ platformę dla korzystania z zawartości (tj. gry, video, film, muzyka, media, włącznie ze społecznościowymi ich rodzajami, tj. chat, etc.). Powinny więc obowiązywać tożsame pryncypia co do istotności efektywnej kontroli rodzicielskiej, realizowanej za pomocą dostarczanych im informacji i odpowiednich narzędzi; podobnie w przypadku klasyfikacji zawartości, opierającej się na standardach aksjologicznych ustanowionych w odnośnych systemach samoregulacyjnych, weryfikowanych pod kątem ich skuteczności[23].

Odpowiedzialne podejście MP oznacza przede wszystkim sprawowanie kontroli nad treściami własnymi lub wykonywanie jej w ramach specjalistycznych zleceń; nie obejmuje się nią natomiast, nie związanej z MP, zawartości darmowo dostępnej w Internecie. Promowanie bezpieczeństwa w korzystaniu przez dzieci i młodszych nastolatków z usług mobilnych wymaga współpracy z klientami, rodzicami, właściwymi organizacjami pozarządowymi poprzez np. kontrolę dostępu do treści przeznaczonych wyłącznie dla osób dorosłych czy oferowanie odpowiednio dostosowanych systemów płatności[24]. Mechanizm kontroli dostępu do określonych treści łączy się raczej z kategoryzowaniem ich według kryterium wieku i polega na dostarczeniu środków ochronnych, umożliwiających rodzicom/ opiekunom nadzór nad nimi; dotyczy to zarówno materiałów własnych, dostarczanych na podstawie umowy, czy wreszcie przez stronę trzecią. Ponadto w ramach indywidualnych umów z użytkownikami MP są odpowiedzialni za umożliwienie rodzicom regulowania dostępu dzieci do usług mobilnych w postaci np. oferowania specjalnych telefonów, filtrów (ograniczających lub blokujących), kontroli bilingów. Drugim celem MP stało się zwiększenie świadomości i edukacja rodziców poprzez: zapewnienie im efektywnego dostępu do informacji i porad, w zakresie użytkowania mobilnych usług telefonicznych i mechanizmów raportowania kwestii związanych z bezpieczeństwem; zachęcanie do prowadzenia rozmów z dziećmi, dostarczanie rodzinom aktualnych materiałów edukacyjnych oraz wspieranie kampanii na rzecz wzrostu świadomości społecznej ich klientów.

Według porozumienia, w kwestii komercyjnej zawartości, dostawcy technologii mobilnych i treści powinni wspierać ramy klasyfikacyjne dla jej oceny, oparte o krajowe standardy prawne i systemy odnoszące się do sektora mediów, na straży których powinny stać zarówno wspomagające je organy władzy publicznej, jak i inne zainteresowane strony. Powinny one składać się co najmniej z dwóch kategorii: 1) odpowiedniej wyłącznie dla osób dorosłych oraz 2) pozostałej, przeznaczonej również dla osób

23) Z uwzględnieniem: *the cross media aspect of content delivery, Tamże.*

24) *Mobile providers offer content which may use pre-pay, post-pay or hybrid approaches to billing (European mobile providers –a responsible approach); Tamże .*

poniżej 18 roku życia; zasady te objęły zarówno treści własne, jak i przekazywane przez dostawców w ramach zawartych umów[25].

MP powinni współdziałać z właściwymi władzami krajowymi w tworzeniu, przyjmowaniu lub egzekucji przepisów i procedur, dotyczących zwalczania treści nielegalnych ujawnionych w urządzeniach mobilnego przekazu; współpraca powinna zachodzić zwłaszcza w ramach tzw. gorących linii (*hotlines*), ułatwiających notyfikację takiej zawartości w zakresie środowiska produktów mobilnych lub w Internecie. Efektywność wymaga klarowności prawnej co do natury treści prawem zakazanych i uprawnień władz publicznych państw członkowskich (lub delegowanych na inne podmioty) co do potwierdzania nielegalności poszczególnych składników zawartości[26]. Wdrażanie krajowych ram klasyfikacyjnych pozwala na uwzględnienie różnic w zakresie moralności publicznej państw członkowskich, co stanowi o odmienności aksjologicznej wpływającej na charakter ich rynków.

3. Program bezpieczniejszego Internetu (2009 – 2013)

Uwzględniając powyżej wskazane inicjatywy, szczególnego znaczenia nabiera fakt, że od 1999 roku Komisja Europejska rozwija kompleksowe podejście, ukierunkowane na stworzenie bezpiecznego internetowego środowiska dla małoletnich w ramach cyklu *Safer Internet Programme.* Do tej pory powstały następujące jego edycje: *Early Programmes* (1999 – 2004), *Safer Internet Plus* (2005 – 2008), *Current Programme* (2009 – 2013)[27]. Mają one na celu: 1) promowanie bezpieczniejszego korzystania z Internetu i innych technologii komunikacyjnych, zwłaszcza w odniesieniu do dzieci i młodzieży; 2) edukowanie użytkowników, w szczegól-

25) Ale: *As pointed out by the GSMA10 Europe in their response to the online consultation, this approach reflects a reality where commercial content available over mobile phones is adapted and rarely produced originally for the mobile format; ibidem*.

26) Por. też: 2010 Implementation report of the European Framework; 2009 Implementation Report of the European Framework, etc. http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework [dostęp: 20.06.2012].

27) Por. *Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors, (the Safer Internet Action Plan 1998-2004); Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies (the Safer Internet plus programme 2005-2008); Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market; Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies* (pkt 3, 6), OJ. EU. L. 348/118, 24.12.2008.

ności osób młodych, rodziców/ opiekunów i nauczycieli oraz 3) zwalczanie nielegalnej lub szkodliwej zawartości Internetu. Można powiedzieć, że programy te ewoluowały i stały się podstawą wielu inicjatyw, stanowiących tzw. wartość dodaną w UE; wykazały też potrzebę podtrzymania dotychczasowych i prowadzenia dalszych działań w zakresie wzrastania świadomości społecznej w sektorze usług *on-line*.

Mimo iż współczesne dzieci i młodzież we wcześniejszym niż poprzednie pokolenia wieku zaczynają korzystać z Internetu, nie jest to jednoznaczne z przyjęciem, że są jego dojrzałymi użytkownikami w rozumieniu rozpoznawania i identyfikowania zagrożeń, na które właśnie one są w szczególności wystawiane; nie można ich zatem pozostawić bez wsparcia w radzeniu sobie z konsekwencjami podejmowanych, nie zawsze w sposób przemyślany, decyzji. Informowanie o ryzyku powinno obejmować środowiska rodzinne, szkołę i samych małoletnich. Zwalczanie nielegalnej i ograniczanie dostępu do potencjalnie szkodliwej zawartości i zdolność odpowiedzialnego zachowania w korzystaniu z usług *on-line* powinno być priorytetem i jest głównym celem prowadzonych w tym obszarze unijnych programów.

Obecna edycja programu powstała w oparciu o decyzję Parlamentu Europejskiego i Rady z 16.12.2008 roku *ustanawiającą wieloletni wspólnotowy program ochrony dzieci korzystających z Internetu i innych technologii komunikacyjnych* (SIP); ustanowiony on został na 5 lat od 1 stycznia 2009 roku. Główną przesłanką jego powstania był znaczący wzrost użytkowania Internetu i innych technologii komunikacyjnych, tj. telefonia mobilna; obecnie z jednej strony zwiększają się szanse, interakcyjność i możliwości kreatywności użytkowników, z drugiej zaś wzmaga i rozszerza zakres dotychczasowych obszarów ryzyka. Pojawiające się coraz to nowe techniczne formy komunikowania zmieniają w istotnym stopniu poglądy i zachowania społeczeństwa informacyjnego; zatem środki ochronne powinny być przyjmowane na poziomie europejskim[28].

Istnieje ciągła potrzeba działania w kwestiach związanych z zagrożeniami Internetu i/albo interaktywnych technologii cyfrowych, włącznie z telefonią mobilną. W szczególności dotyczy to wykorzystywania dzieci i przeciwdziałania ich wiktymizacji w związku ze szkodliwą lub nielegalną zawartością (tj. np. pornografia). Nacisk powinien zostać położony na po-

28) *The Commission Communication 'i2010 — A European Information Society for growth and employment'* COM(2005)0229*), developing the Lisbon strategy, seeks to ensure coherence across the Commission's information society and media policies in order to reinforce the significant contribution of information and communication technologies to the performance of the economies of Member States. One of its objectives is the creation of a Single European Information Space offering affordable and secure high bandwidth communications, rich and diverse content, and digital services; Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce),* Ibidem, pkt 2 i 3.

szukiwanie rozwiązań w zakresie przeciwdziałania składania, za pomocą technologii komunikacyjnych, przez osoby dorosłe dzieciom propozycji o charakterze seksualnym; problemem jest także kierowanie przeciwko małoletnim gróźb, nękanie ich czy upokarzanie.

Zmieniający się krajobraz medialny, powstający w wyniku rozwoju technologii komunikacyjnych i innowacji medialnych, zmienia zachowania społeczne i wywołuje nowe rodzaje ryzyka dla dzieci. Poznanie zagrożeń i rozumienie ich istoty wymaga permanentnego uczenia dzieci, rodziców, opiekunów, etc. korzystania z usług *on-line* w sposób efektywny i bezpieczny; program powinien zatem zawierać odpowiednie pakiety edukacyjne, odnoszące się np. do rozwijania skutecznych systemów kategoryzacji wiekowej czy klasyfikacji treści. Różnorodne środki i działania powinny być łączone w sposób wzajemnie się uzupełniający i spójny, promujący bezpieczeństwo i odpowiedzialność, dobre praktyki i odpowiednie standardy zachowań; współpraca powinna być prowadzona na wszystkich poziomach i z udziałem wszystkich zainteresowanych stron (zwłaszcza przedstawicieli odnośnych przemysłów). Za komplementarność i synergię programów i inicjatyw na poziomie unijnym i międzynarodowym, z uwagi na globalny wymiar problemu, odpowiada Komisja Europejska, działająca poprzez struktury sieci, uwzględniające transgraniczne zagrożenia pochodzące z państw trzecich[29]. Skuteczność przyjmowanych rozwiązań wymaga zatem ich kształtowania na poziomie ponadnarodowym, z uwagi na potencjalną kolizję praw, uwzględniającym zastosowanie zasady subsydiarności[30].

1. Celami obecnego programu 'Bezpieczniejszy Internet' są głównie: 1) rozwijanie świadomości publicznej co do bezpieczeństwa sfery nowych technologii, 2) szeroko rozumiana promocja bezpiecznego środowiska *on-line*, 3) zwalczanie nielegalnej zawartości i szkodliwego postępowania,

---

29) *Illegal content may be produced in one country, hosted in a second, but accessed and downloaded worldwide.*

30) Program cechuje się otwartą formułą. Zgodnie z art. 2 mogą brać w nim udział osoby prawne pochodzące zarówno z państw członkowskich UE, EFTA, EEA, krajów kandydujących, znajdujących się w procedurze akcesji do UE, reprezentujących region zachodnich Bałkanów i sąsiadujących z Unią oraz z państw trzecich – stron międzynarodowych porozumień ze Wspólnotą; pod pewnymi warunkami dopuszczalne jest także uczestnictwo organizacji międzynarodowych i osób prawnych ustanowionych w innych państwach trzecich. Instytucją odpowiedzialną za implementację programu jest Komisja Europejska, działająca w ścisłej współpracy z państwami członkowskimi, zapewniając jednocześnie komplementarność z innymi właściwymi, unijnymi programami i inicjatywami (art. 3); odpowiada ona także ze efektywne wykorzystanie środków finansowych w kierunku zapewnienia zgodnego z decyzją wykonywania poszczególnych działań oraz za monitorowanie wdrażania projektów przyjętych na mocy programu; por. też: Annex II *Indicative breakdown of expenditure - (1) Ensuring public awareness 48 %; (2) Fighting against illegal content and harmful conduct online 34 % (3) Promoting a safer online environment 10 % (4) Establishing a knowledge base 8 %.*

4) ustanowienie niezbędnej bazy danych[31] o nowych tendencjach korzystania z Internetu i ich konsekwencjach dla życia dzieci.

Aneks I precyzuje zadania w obrębie powyżej wymienionych grup celów.

Rozwijanie świadomości publicznej, głównie wśród użytkowników końcowych (dzieci, rodziców/ opiekunów, nauczycieli i pedagogów) ma charakter ogólnounijny i polega na przekazywaniu wiedzy na temat szans i zagrożeń oraz środków bezpieczeństwa w nowym środowisku *on-line*, platform dystrybucyjnych (tj. usługi audiowizualne poprzez mobilne sieci telekomunikacyjne); proponuje się następujący pakiet działań:

a) rozpowszechnianie, przede wszystkim we współpracy i za pomocą środków masowego przekazu, czy poprzez system edukacyjny lub w bezpośredniej dystrybucji do użytkownika, odpowiednich informacji na temat bezpiecznego korzystania z technologii on-line, dla szerokiego kręgu użytkowników, ze zindywidualizowaniem grup docelowych (np. ustalanych według kryterium wieku);

b) wprowadzenie punktów kontaktowych, w których rodzice i dzieci mogą otrzymywać odpowiedzi na problemy związane z bezpieczeństwem on-line, porady, w jaki sposób reagować np. na uwodzenie, nękanie czy ośmieszanie małoletnich; sprzyja to odpowiedzialnym wyborom opartym na właściwych przesłankach;

c) zachęcanie do stosowania efektywnych długoterminowo metod i narzędzi dla zwiększania się świadomości społecznej;

d) unijną i międzynarodową wymianę dobrych praktyk, informacji, metod, narzędzi i doświadczeń dla prowadzenia efektywnej współpracy, doskonalenia i poprawiania, także związanej z kosztami, skuteczności i zwiększania zasięgu globalnych inicjatyw.

Niejako uzupełnieniem powyższych działań jest promowanie w ramach współpracy zainteresowanych stron, bezpiecznego środowiska *on--line*; zaplanowano następujące działania:

a) utworzenie otwartej platformy dyskusyjnej łączącej promowanie bezpieczeństwa i sposobów ochrony dzieci przed potencjalnie szkodliwą zawartością przedstawianą na różnych płaszczyznach technologicznych dla poprawienia współpracy, wymiany informacji, doświadczeń i dobrych praktyk między zainteresowanymi stronami oraz zharmonizowanie podejść w kreowaniu bezpiecznego środowiska dla dzieci;

b) zachęcanie zainteresowanych stron do tworzenia, rozwijania i wdrażania odpowiedniego systemu samo- i koregulacyjnego przy uwzględnieniu w rozwijaniu nowych technologii bezpieczeństwa dzieci;

c) wspieranie dostawców usług internetowych w rozwijaniu bezpiecznego oznakowania treści poszczególnych witryn internetowych, czy

31) Pojęcie to trzeba traktować jako obejmujące szeroką wiedzę, informacje o bezpieczeństwie środowiska *on-line*.

podstron, jako narzędzi samoregulacyjnych oraz poszukiwanie możliwości ustanowienia wspólnego systemu opisowych symboli lub ostrzeżeń, wskazujących na określone kategorie wiekowe małoletnich lub na aspekty warunkujące czy dana zawartość jest, czy nie rekomendowana dla poszczególnych subkategorii[32];

d) stymulowanie, przy wsparciu specjalistów w obszarze bezpieczeństwa nowych technologii dla małoletnich, zaangażowania dzieci w kreowanie bezpiecznego środowiska *on-line*, z zapewnieniem zasad niedyskryminacyjnych, jeśli chodzi o płeć, ukierunkowanych na lepsze rozumienie ich poglądów i doświadczeń[33];

e) zwiększanie informacji dla rodziców/ opiekunów, nauczycieli, etc. o odpowiednio skutecznych, wspierających narzędziach dla radzenia sobie ze szkodliwą zawartością *on-line* występującą na różnych platformach, poprzez regularne wyposażanie wszystkich użytkowników w proste materiały edukujące, instrumenty i aplikacje, tj. systemy filtrujące;

f) zapewnianie kompatybilności podejść międzynarodowych i na poziomie Unii Europejskiej, opartych o promowaną kooperację, wymianę doświadczeń, informacji, dobrych praktyk między zainteresowanymi stronami.

W zakresie celu trzeciego, ukierunkowanego na redukcję treści nielegalnych krążących w sieci i odpowiedniego radzenia sobie z materiałami o szkodliwej dla małoletnich zawartości, dystrybuowanymi *on-line*, powstało pytanie o metodę zwalczania: 1) niegodziwego traktowania dzieci, 2) psychologicznej manipulacji nimi w kontekście ich wykorzystywania seksualnego (włącznie z nakłanianiem do prostytucji czy pornografii), poprzez uwodzenie przez Internet, nawiązanie przyjaźni, bliskości uczuciowej czy emocjonalnej (*grooming*), 3) nękania, prezentowania psychicznej lub fizycznej agresji (*cyberbulling*).

Istotne jest tu zapewnienie świadomości społecznej o zagrożeniach i ich przesłankach oraz edukacja i pomoc użytkownikom końcowym (głównie dzieciom, rodzicom/opiekunom, nauczycielom i pedagogom) poprzez partnerską współpracę zainteresowanych stron i uzyskanie koherentnego podejścia względem zawartości usług *off-line* i *on-line* wydaje się kluczowe; zaproponowano następujące główne inicjatywy:

a) szerokie informowanie opinii publicznej o istniejących punktach kontaktowych i tzw. gorących liniach, raportujących o zawartości niele-

32) Podstawą jest tu system PEGI *on-line*. W ramach jednego z projektów programu bezpieczniejszego internetu – Quatro Plus uwzględnia się opinie użytkowników końcowych co do rodzaju proponowanych oznakowań, http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2006-UE-211001 (26.06.2012).

33) Por. np. *The European Forum on the Rights of the Child,* za: http://ec.europa.eu/justice/fundamental-rights/rights-child/european-forum/index_en.htm (20.06.2012); *The Safer Internet Forum,* za: http://ec.europa.eu/information_society/activities/sip/events/forum/index_en.htm (20.06.2012).

galnej i szkodliwych zachowaniach. Punkty te powinny być znane publicznie i powiązane z właściwymi podmiotami krajowymi (np. z jednostkami policji specjalizującymi się w cyberprzestępczości i współpracującymi na poziomie unijnym w rozwiązywaniu transgranicznych problemów); powinny też przekazywać niezbędne informacje o sposobach informowania o zawartości nielegalnej i klasyfikacjach usług informacyjnych *on-line*, potencjalnie zagrażających prawidłowemu rozwojowi małoletnich;

b) blokowanie wyżej omawianych, szkodliwych zachowań *on-line*, poprzez działania techniczne, psychologiczne i socjologiczne, koordynowane na poziomie współpracy między zainteresowanymi stronami;

c) stymulowanie aplikowania efektywnych narzędzi technicznych dostosowanych do zwalczania nielegalnej zawartości szkodliwych zachowań i informujących użytkowników końcowych o sposobach ich bezpiecznego i odpowiedzialnego użytkowania; w szczególności powinny być one łatwe do obsługi, dostępne bez opłat i szeroko promowane przez operatorów usług. Postuluje się stosowanie *inter alia* następujących środków: (1) przyjęcie „znaków" jakości dla dostawców usług, pozwalających użytkownikom w łatwy sposób powziąć informację o stosowaniu lub nie przez konkretny podmiot dobrych praktyk; (2) korzystanie przez użytkowników końcowych z filtrów *on-line*, zapobiegających materiałom potencjalnie szkodliwym; (3) wspieranie i promowanie środków zachęcających do tworzenia wartościowych dla dzieci treści; (4) poszukiwanie, we współpracy z przemysłem internetowym, skutecznych narzędzi umożliwiających organom egzekucyjnym śledzenie *on-line* przestępców;

d) promowanie kooperacji, wymiany informacji, doświadczeń i dobrych praktyk pomiędzy zainteresowanymi stronami na poziomie krajowym i unijnym, w tym na poziomie rządów, organów wymiaru sprawiedliwości, przedstawicieli przemysłu internetowego, banków, a także tzw. gorących linii i organizacji pozarządowych, zajmujących się niniejszą problematyką;

e) położenie nacisku na kooperację, wymianę informacji i doświadczeń w zakresie zwalczania treści nielegalnych i szkodliwych zachowań na poziomie międzynarodowym. Szczególnego znaczenia nabiera polepszenie współpracy z krajami trzecimi, w tym przyjmowanie zharmonizowanych, na poziomie międzynarodowym, podejść do problemu. Kraje członkowskie zostały zobowiązane do rozwijania, współpracy wzajemnej i w ramach Europolu, w związku z istniejącymi na ich terytoriach bazami danych, dotyczącymi wykorzystywania dzieci oraz przyjmowania wspólnego podejścia, na podstawie bliskiej współpracy pomiędzy krajowymi władzami, policją i punktami kontaktowymi;

f) połączenie, o ile jeszcze nie funkcjonują, rejestrów domen państw członkowskich oraz wzmocnienie istniejącej kooperacji i zachęcanie do jej rozszerzania na kraje trzecie, w celu wczesnego wykrywania

potencjalnie nielegalnej zawartości i minimalizowania czasu obecności w sieci witryn (czy podstron) zawierających treści o seksualnym wykorzystywaniu dzieci.

Stworzenie bazy, obejmującej całokształt zagadnień związanych z bezpieczeństwem środowiska *on-line,* pozwala na wymianę wiedzy między zainteresowanymi stronami, rozpowszechnianej w państwach członkowskich; główne działania koncentrują się na:

a) zachęcaniu do, koordynowanej na poziomie UE, międzynarodowej współpracy naukowców, ekspertów, etc. zaangażowanych w problematykę bezpieczeństwa dzieci *on-line* poprzez np. uaktualnianie przeglądów istniejących i nowopojawiających się badań w celu wypracowywania wspólnych podejść do omawianej problematyki;

b) dostarczaniu aktualizowanych informacji na temat korzystania przez dzieci z nowych technologii *on-line*, z uwzględnieniem danych, jak radzą sobie one, ich rodziny i otoczenie szkolne z pojawiającymi się szansami i zagrożeniami, w tym jakie małoletni proponują własne strategie i jak należy ocenić ich efektywność;

c) analizowaniu statystyk i trendów występujących w krajach członkowskich w celu umożliwienia odpowiednim organom ich władz publicznych zredukowania sytuacji dublowania wysiłków i jednocześnie maksymalizacji wykorzystania istniejących sił i środków;

d) promowaniu śledzenia technicznych, psychologicznych i socjologicznych kwestii, związanych z wiktymizacją dzieci *on-line*, włączając w to zarówno – omawiane wyżej – wykorzystywanie dzieci (w tym seksualne), jak i nowopojawiające się formy zachowań, narażające je na pokrzywdzenie/ poszkodowanie;

e) promowaniu analizowania efektywnych sposobów, metod i narzędzi ulepszania bezpieczeństwa środowiska *on-line*, tj. systemy samo- i koregulacyjne, techniczne zabezpieczenia i inne rozwiązania;

f) rozwijaniu wiedzy na temat korzystania przez dzieci z nowych technologii; analizowaniu psychologicznego i socjologicznego oddziaływania środowiska *on-line* na poglądy i zachowania małoletnich, począwszy od skali zagrożeń, po ich zakres, obejmujący różne platformy (od komputerów i telefonów komórkowych, przez konsole do gier i inne nowe technologie, z uwzględnieniem podejścia w zależności od płci użytkownika/konsumenta)[34].

34) Należy tu zwrócić uwagę na inicjatywę *Safer Internet Forum* – coroczną, europejską konferencję skupiającą przedstawicieli odpowiednich: władz publicznych, przemysłu i organizacji pozarządowych, której celem jest wymiana doświadczeń i wiedzy w ramach krajowych ciał samo- i koregulujących, w zakresie wkładu przemysłu w kreowanie bezpieczniejszego dla dzieci środowiska nowych technologii (zwalczanie nielegalnej treści, także stanowiącej przestępstwa przeciwko najmłodszym, http://ec.europa.eu/information_society/newsroom/cf/itemdetail.cfm?item_id=6000&utm_campaign=isp&utm_

Unia działa poprzez Centra (*Safer Internet Centres*); są one obecne w 30 krajach europejskich i ukierunkowane na uświadamianie dzieciom, rodzicom/opiekunom i nauczycielom zagrożeń występujących w środowisku *on-line* i oferowanie porad w zakresie bezpieczeństwa dzieci i młodzieży, za pośrednictwem tzw. linii pomocowych *(help lines*) i tzw. punktów kontaktowych (*contact points – hotlines*), służących informowaniu o nielegalnych treściach. Centra uwzględniają specyficzne narodowe odniesienia i wrażliwość; ich działalność ma też wymiar międzynarodowy, zwłaszcza w zakresie zwalczania nielegalnej zawartości[35].

W lutym 2012 roku przedstawiono raport ogólnie pozytywnie oceniający skutki realizacji podstawowych celów omawianego programu w pierwszych

---

medium=rss&utm_source=newsroom&utm_content=tpa-129 [dostęp: 26.06.2012]; por. też: inicjatywę *Safer Internet Day,* organizowany przez INSAFE, http://www.saferinternet.org/web/guest/safer-internet-day [dostęp: 20.06.2012]; czy *Youth Panel* organizowany przez *Safer Internet Centres, http*://ec.europa.eu/information_society/activities/sip/projects/centres/panels/index_en.htm [dostęp: 20.06.2012].

35) Polskie centrum jest zorganizowane i koordynowane przez Naukową Akademicką Sieć Komputerową i fundację „Dzieci Niczyje" od 2005 roku, http://www.saferinternet.pl/safer_internet_w_polsce.html [dostęp: 20.06.2012]; prowadzi: Saferinternet.pl – kompleksowe inicjatywy, mające na celu szreokie uświadamianie zagrożeń *on-line*; helpline.org.pl – działania wspierające i poradnicze dla małoletnich i ich rodziców/opiekunów, http://www.helpline.org.pl [dostęp: 20.06.2012]; dyżurnet.pl – ukierunkowane na usunięcie internetowych treści nielegalnych, wytworzonych z udziałem dzieci lub skierowanych przeciwko ich bezpieczeństwu http://dyzurnet.pl/zglos_nielegalne_tresci_ref.php [dostęp: 20.06.2012]; por. też:: http://ec.europa.eu/information_society/activities/sip/projects/centres/index_en.htm [dostęp: 20.06.2012].

Telefony świadczące pomoc *(help lines)* – ukierunkowane na oferowanie szerokich porad w obszarze bezpieczeństwa *on-line* dla młodych osób, ich rodzin i profesjonalistów; od 2008 roku działa sieć *hot lines* ustanowiona w 26 państwach członkowskich UE i spoza Europy (Australia, Kanada, USA, Japonia, Płd Afryka, Korea, Tajwan i Rosja) w celu otrzymywania raportów krajowych na temat nielegalnej zawartości *on-line* i zwalczania wykorzystywania dzieci (INHOPE). Ponadto należy zwrócić uwagę na INSAFE – paneuropejską sieć, obejmującą centra informacyjne (*awarness centres*) i tzw. linie pomocy (*help lines*), ukierunkowaną na rozwijanie materiałów i kampanii informacyjnych i organizującą takie wydarzenia jak *Safer Internet Day* czy inicjatywy, tj. panele dla młodych (*youth panel*); por. też: – europejska sieć punktów kontaktowych dla raportowania o nielegalnej i szkodliwej treści w Internecie (*hotline*s*);* EU.kidsonline http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx.

Kolejnymi projektami są: 1) CIRCAMP, ukierunkowany na zwiększenie efektywności międzynarodowych działań policyjnych, http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2007-TN-140701 [dostęp: 20.06.2012];

2) MAPAP, ukierunkowany na zwalczanie pedofilów, a szerzej materiałów wykorzystujących dzieci i innej szkodliwej zawartości w systemie peer-to-peer (p2p), m.in. w drodze korzystania z odpowiednich filtrów; 3) I-Dash – służący zwalczaniu zwiększającej się liczby 'wideo kolekcji', zawierających sceny seksualnego wykorzystywania dzieci, poprzez współpracę policyjną ustanowienie multilateralnego modelu wymiany informacji w tym zakresie, 4) FIVES, rozwijający narzędzia koncentrujące się na szybkiej i efektywnej pomocy w śledztwach policyjnych, ukierunkowanych na analizowanie zawartości (obrazy i wideo) odnoszącej się do wykorzystywania dzieci, za: http://ec.europa.eu/information_society/activities/sip/projects/completed/illeg_content/index_en.htm [dostęp: 20.06.2012].

latach jego trwania w zakresie wspólnych, koordynowanych przez UE działań chroniących dzieci w świecie Internetu i stale pojawiających się nowych technologii i form komunikacyjnych[36]. Niektóre jednak kwestie wymagają rekomendacji do dalszych działań[37]. I tak widać potrzebę ściślejszego włączenia organizacji międzynarodowych i reprezentujących odnośny przemysł w aktualne inicjatywy; aktywność pojedynczych, niezorganizowanych podmiotów nie jest tak efektywna. Obecnie nacisk powinien zostać położony na wspieranie rozwoju bazy informacyjnej i badań naukowych.

Sprawność wdrażania SIP oceniana jest wysoko, ale postuluje się, sprzyjające bardziej elastycznym gospodarowaniem funduszami, dłuższe okresy rozliczeniowe; kluczowym problemem mogą się tu jednak okazać cięcia budżetowe w krajach uczestniczących. Merytorycznie najważniejszym elementem jest funkcjonowanie formalnych i nieformalnych sieci pomiędzy projektami i szerzej zainteresowanymi stronami; dobrze ocenia się koordynację różnych programów prowadzonych przez KE w tym obszarze. Osiągnięciem SIP jest istnienie w większości państw członkowskich UE tzw. gorących linii (*hotlines*), linii oferujących pomoc (*helplines*) czy swoistych centrów informacyjnych rozwijających świadomość społeczną (*awarness centres*); również uczestnictwo różnorodnych podmiotów ma istotne znaczenie dla skuteczności programu, poprzez wymianę i zbalansowanie poglądów i impet w realizacji programu.

Odnośnie ciągłości i wpływu SIP wskazuje się, że obecne jego kierunki i struktura są właściwe i nie wymagają istotnych zmian, tym bardziej że nie koncentruje się on już zasadniczo na poszukiwaniu technicznych rozwiązań. Biorąc pod uwagę, że niektóre zagadnienia nim obejmowane odnoszą się do tzw. szarych stref, konieczna jest dobra wiedza na temat krajowych kontekstów regulacyjnych; nadal powinno się podnosić świadomość społeczną i wzmacniać bliższą współpracę. Komisja Europejska zaproponowała pakiet rekomendacji, ukierunkowanych jednak nie na rozszerzanie celów, a raczej na kontynuowanie dotychczasowych wysiłków w ochronie dzieci w formule długoterminowych strategii. Proponuje się poprawienie bazy wiedzy, sprzyjającej istniejącym i nowym powią-

36) Podkreśla się, że program istotnie wpływa na działania zarówno krajowe, jak i międzynarodowe; *Interim evaluation of the multi-annual Community programme on protecting children using the Internet and other communication technologies,* version 1.1 28 February 2011, SMART 2009/0042/lot 2 – Final report, za; http://ec.europa.eu/information_society/activities/sip/docs/prog_2009_2013/FINAL%20REPORT%2020120124.pdf [dostęp: 26.06.2012]; por. też: *Background report on age verification, cross media rating and calisfication and age veryfication solutions* (2008), Safer Internet Forum 25 – 26 September 2008, http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf [dostęp: 26.06.2012].

37) Na przykład, odnosząc się do nowych zjawisk, szczególną uwagę należy zwrócić na media społecznościowe i nękanie (*cyber bullying)* i w tym kontekście zaproponować strategie odnośnie np. prawa do prywatności.

zaniom między reprezentantami przemysłu, organizacji międzynarodowych, dostawców treści, producentów technologii, etc.; postuluje się zorganizowanie debaty o włączeniu dzieci bezpośrednio do programu.

W zakresie wydajności programu proponuje się, poza wspomnianym wyżej wydłużeniem okresów finansowych, rozważenie wprowadzenia wspólnych z innymi dyrekcjami (wydziałami – tj. sprawiedliwości, spraw wewnętrznych, edukacji czy kultury) projektów wykorzystujących istniejące kanały komunikacyjne. Przewiduje się koordynowanie inicjatyw w ramach tzw. gorących linii (*hot lines*), telefonów pomocowych (*help lines*) i informacyjnych centrów uświadamiających (*awareness centres*); podkreślono, że już obecnie występuje współpraca pomiędzy INHOPE i INSAFE, a oczekuje się włączenia INTERPOL-u.

W odniesieniu do efektywności ważne jest: 1) uświadomienie na poziomie krajowym ważności programu i potrzeby jego realizacji, 2) rozwijanie metod kształtujących spójne zobowiązania odnośnego przemysłu, poprzez korporacyjną odpowiedzialność lub debatę na temat prawnych aspektów ochrony małoletnich, 3) rozwój możliwości wynikających z funkcjonowania międzynarodowych sieci, 4) wspieranie rozszerzania bazy wiedzy, coroczne raportowanie wyników programu, z uwzględnieniem kwestii włączania go w ramy programów szkolnych. W zakresie oddziaływania ciągłości programu rozważenia wymagają: 1) ustanowienie forów dyskusyjnych na tematy: rozwoju nowych technologii, prawnych ich regulacji, etc.; 2) poprawienia koherentnej komunikacji i oceny wpływu inicjatyw podejmowanych w jego ramach i z uwzględnieniem ich adekwatności do określonych grup adresatów[38].

4. Ochrona małoletnich w środowisku *on-line*. Wyzwania dla rodziców

Niniejsze opracowanie poświęcone kwestii ochrony dzieci i młodzieży przed negatywnym wpływem nowych technologii komunikacyjnych w świetle dokumentów Unii Europejskiej obejmuje okres 1996 – 2012. Program *Safer Internet* i zalecenia zawarte w innych, omawianych wyżej, dokumentach kieruje w istocie swoje projekty do użytkowników końcowych, tj. rodziców, nauczycieli, dzieci i młodzieży, bowiem to właśnie od nich zależy jego efektywność. Szczególną rolę pełnią tu opiekunowie

38) Por. np. 1) program Komisji Europejskiej Daphne, ukierunkowany na zapobieganie i zwalczanie przemocy wobec dzieci, młodzieży i kobiet oraz ochrona ofiar i grup narażonych na szczególne ryzyko, za: http://ec.europa.eu/justice_home/daphnetoolkit/html/welcome/dpt_welcome_en.html [dostęp: 27.06.2012], 2) program Komisji Europejskiej Media literacy poświęcony kwestiom kompetencji w zakresie dostępu oraz rozumienia krytycznego podejścia i umiejętności kreowania współczesnego środowiska mediów, za: http://ec.europa.eu/culture/media/literacy/index_en.htm , [dostęp: 27.06.2012].

małoletnich, praktycznie odpowiedzialni za uniemożliwianie lub ograniczanie im dostępu do treści prawem zakazanej lub szkodliwej. Ich znaczenie Unia Europejska dostrzegała już w latach 90. ubiegłego wieku. Wówczas bowiem zbadano pod tym kątem realizację art. 22b dyrektywy 97/36/EC „o telewizji bez granic", obejmującą kwestię kontroli rodzicielskiej w zakresie tradycyjnego rozpowszechniania telewizyjnego. W wydanym 19. 07. 1999 r. komunikacie *Studium w sprawie kontroli rodzicielskiej w rozpowszechnianiu telewizyjnym*[39] uwzględniono zwłaszcza europejskie doświadczenia zainteresowanych stron oraz rozważano stopień implementacji i efektywności następujących wymaganych metod i środków: 1) wyposażenia odbiorników telewizyjnych w urządzenia techniczne umożliwiające rodzicom/opiekunom filtrowanie programów; 2) ustanowienia systemów oznakowania; 3) zachęcenia do prowadzenia w tym zakresie odpowiedniej polityki rodzinnej i innych metod uświadamiających czy edukacyjnych. Już wówczas podkreślano, że potencjalna szkodliwość zawartości audiowizualnej stanowi istotne zagrożenie dla interesu publicznego, dlatego ochrona małoletnich odbiorców, bardziej narażonych na ryzyko odbierania niewłaściwych dla nich treści, powinna zostać zapewniona.

Wnioski wynikające z omawianego studium są adekwatne także w warunkach nowych, zglobalizowanych technologii, bo odzwierciedlają one zmianę podejścia do problematyki w związku z zachodzącym procesem digitalizacji[40]. Zwrócono uwagę na rozszerzający się zakres dostępnych transgranicznie kanałów telewizyjnych, co utrudniało ich monitorowanie, zwłaszcza jeśli wziąć pod uwagę, że powszechnie stosowane w USA i Kanadzie 'V-chipy' okazały się technicznie niemożliwe do zastosowania w Europie. Wymagało to więc wprowadzenia otwartych na technologie cyfrowe, niezawodnych i bezpiecznych systemów filtrowania, w szczególności względem kodowanych usług, takich jak *pay-TV, pay-per-view* i *video on demand*, jednak niezunifikowanych, bo odzwierciedlających różnice w kulturowych i aksjologicznych systemach obowiązujących w poszczególnych państwach członkowskich. Równie ważne było przyjęcie systemów oznakowań dla paneuropejskich audiowizualnych usług medialnych, co było również utrudnione znacznymi odmiennościami tradycji krajowych i w indywidualnym podchodzeniu do kwestii moralności publicznej. Osadzenie we własnej kulturze, obyczajowości i ich historycznych fundamen-

39) *Commission Communication on the* Study on Parental Control of Television Broadcasting (1999), Brussels, 19/07/99 COM/99/371 final; por. też European Parliament resolution on the Commission communication "Study on Parental Control of Television Broadcasting" (COM(199) 371- C5-0324/1999); Commission Communication : Combating trafficking in human beings and combating the sexual exploitation of children and child pornography, COM(2000)854 final, [dostęp: 21.12.2000].

40) Odwołanie do: *Decision 276/1999/EC of The European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet by combating illegal and harmful content on global networks.*

tach, jako istotny element tożsamości narodowej, stanowi niewątpliwą wartość w UE; z drugiej jednak strony komplikuje to w pewien sposób uzyskiwanie spójnych efektów. W takiej sytuacji wymóg zachowania pluralistycznego podejścia skutkował wątpliwościami co do efektywności podejmowanych środków. Zdecydowano więc o wprowadzeniu na poziomie europejskim ogólnych deskryptywnych kryteriów, których ocena należeć powinna do krajowych lub regionalnych regulatorów, w oparciu o precyzyjne i transparentne wyznaczniki, wyjaśniające podstawy ich stosowania. Takie podejście ułatwia europejską współpracę państw członkowskich w uzyskiwaniu, nawet przy zastosowaniu różnych technik, konsekwentnej i spójnej ochrony przed potencjalnie szkodliwymi dla małoletnich treściami; pozwala także na bardziej koherentne ukształtowanie systemów oznakowań przeznaczonych dla różnego charakteru rodzaju mediów: kina, telewizji, gier wideo. Już wówczas położono też nacisk na kwestie szeroko rozumianej edukacji medialnej.

We wnioskach skoncentrowano się na technicznych aspektach dalszej współpracy w ramach *Digital Video Broadcasting (DVB) Project,* obejmującego szeroko rozumiane podmioty sektora audiowizualnego (od rad klasyfikujących filmy, poprzez nadawców, operatorów Internetu, przedstawicieli przemysłu wideo po państwa członkowskie, widzów, użytkowników, etc.); operowano w zakresie, odpowiadającej rzeczywistości cyfrowej, problematyki klasyfikacji zawartości oraz towarzyszących im metod edukacyjnych.

W wyniku tego projektu we wrześniu 2000 roku powstało kolejne, kompleksowe opracowanie *Parental Control in a Converged Communications Environment Self-Regulation, Technical Devices, and Meta-Information*[41] ukierunkowane na ochronę małoletnich przed potencjalnie szkodliwymi treściami prezentowanymi w środowisku nowych technologii.

W jego konkluzjach podkreślono szerokie rozpowszechnianie przez organa władzy publicznej, czy zainteresowane organizacje (reprezentujące np. przemysł czy konsumentów) systemów filtrowania niewłaściwej zawartości. Nacisk miał zostać położony na podmioty funkcjonujące poza centralnym systemem kontroli państwowej; ich efektywność napotyka na poważne trudności uwarunkowane zwiększającymi się rozmiarami oferty o charakterze międzynarodowym, komplikującej – co oczywiste – kwestie ustalania i realizowania indywidualnej jurysdykcji krajowej w tej materii. Uznano zatem, że uwagę należy skoncentrować na wymiarze jednostkowym. Dostępne ówcześnie tzw. pośrednie systemy oznakowania pozwalały nadawcom komercyjnym, dostawcom filtrującego oprogramowania czy in-

41) Por.: *DVB Parental Control Report* October 2000 *Annex B to 001213_DT5634 Parental Control in a Converged Communications Environment Self-Regulation, Technical Devices, and Meta-Information*; the European Commission (EC) asked the Programme in Comparative Media Law and Policy (PCMLP) at Oxford University to conduct this study on Parental Control in Television Broadcasting. This report is limited to harmful content.

nym podmiotom powołanym w celu oceniania zawartości na przekazywanie rodzicom komunikatu o odpowiedniości danych treści dla określonej kategorii wiekowej (np. powyżej 16 roku życia) poprzez EPG lub widoczne na ekranie ikony. Można więc powiedzieć, że istotą tych systemów stało się ostrzeganie opiekunów dzieci o możliwych zagrożeniach; samo zaś niejako wykonanie tej ochrony polegało już na tradycyjnych środkach rodzicielskich, uniemożliwiających małoletnim dostęp do niewłaściwych treści (z wykorzystaniem lub nie technicznych możliwości blokowania takich materiałów). Nowym, rozpatrywanym modelem był filtr konsumencki oparty o opisowe oznakowania zawartości, stanowiące podstawę do jej filtrowania w zależności od decyzji konsumenta. W obydwu tych przypadkach rodzice musieli polegać na ocenach zawartości dokonywanych przez strony trzecie, przy czym w pierwszym z nich dysponowali oni ostrzeżeniem o niewłaściwości danego materiału dla dzieci poniżej określonego wieku, w drugim zaś sami podejmowali decyzję o kategoryzacji wiekowej na podstawie opisu treści, co pozwalało w większym stopniu zindywidualizować postrzeganie zawartości w zależności od tradycji kulturowych, obyczaju, etc. zarówno na poziomie europejskim, jak i międzynarodowym. Dlatego w konkluzji optuje się raczej za drugą prezentowaną powyżej możliwością, co jednakowoż nie wyklucza stosowania innych rozwiązań; w zdigitalizowanym, konwergentym środowisku lepiej sprawdzają się modele zdecentralizowane[42].

Wskazano, że dostosowane do warunków, ówczesne modele systemów filtrujących wymagają spełniania następujących warunków: 1) przyjęcia odpowiedniej terminologii dotyczącej oznakowania – bądź ogólnie informującej, czy dany materiał jest, czy też nie jest właściwy dla określonych kategorii wiekowych dzieci czy młodzieży, bądź precyzyjniej opisujący

42) 1.1. Filtering Typologies: A Continuum *There remain large differences in both technologies and regulatory expectations of content control between the broadcasting and Internet context. Nevertheless, in extremely broad terms, three basic typologies of control can be distinguished. These typologies represent a continuum. At one extreme, regulation is centralised and consumers have minimal access to metainformation about content. At the other extreme, central regulation becomes unnecessary because consumers can carry out their own filtering and control content. The shift toward the latter paradigm is dependent on new technologies: the more that content packagers can (a) provide detailed metainformation about content and (b) give consumers technical options for blocking based on this information, the more control and responsibility can shift to the consumers. A second trend reinforces the same trajectory; as volume of content increases, content packagers' ability to monitor and control distribution may decline and as the number and geographic distribution of content producers increases, the power of any central authority to control content declines.*
1.1.1. Central Regulation – parental digital Central Regulation is most understandable within the historical broadcasting context, and remains the norm for broadcasting in most countries today. Under a central regulation model, a single standard determines what content may be broadcast at any given time. This mode of regulation is only possible where relatively few entities have the power to transmit material, and all of those entities are susceptible to enforcement measures by a regulating body. This mode of control is not feasible for the Internet.

samą treść (np. zawierający sceny nagości, przemocy, etc.)[43]; 2) wyznaczenia przynajmniej jednego podmiotu odpowiedzialnego za przegląd zawartości i wyznaczanie określonych systemów jej kategoryzowania[44]; 3) rozwijania technicznych środków dostarczających rodzicom informacji o dokonywanych klasyfikacjach, co powinno następować w formatach ułatwiających automatyczne blokowanie niepożądanych treści; 4) wdrażania filtrów ukierunkowanych na umożliwienie dokonywania kontroli zawartości przez dorosłych użytkowników – poprzez dostarczanie i stosowanie spójnej terminologii, pozwalającej na automatyczne relegowanie nieodpowiednich materiałów, stanowiącej bądź integralny lub związany z bezpośrednią transmisją, bądź odrębny przekaz omawianych informacji. Jako że opowiadano się raczej za systemem indywidualnych decyzji rodzicielskich niż punktowym instalowaniem filtrów w strumieniowym przepływie informacji, kwestie terminologiczne okazały się kluczowymi dla uzyskania oczekiwanego poziomu ochrony. Projektant systemu filtrującego staje się w takiej sytuacji odpowiedzialny za stworzenie zarówno spójnego języka opisującego treść, jak i odpowiadającego mu systemu opcji blokowania albo akceptowania nieklasyfikowanej zawartości. Co więcej, cyfryzacja, umożliwiająca znacznie większy przepływ informacji, pozwala na przekazywanie opiekunom wystarczająco szczegółowych danych dla podjęcia zdecentralizowanych i zdywersyfikowanych decyzji, uwzględniających indywidualne kulturowe czy ideologiczne preferencje rodzin; oznacza to w praktyce możliwość uzyskania wyższego poziomu ochrony małoletnich. Szczególnie przydatnym narzędziem weryfikacji treści, także pod kątem jej szkodliwości dla małoletnich (np. pornografii) i możliwości ich blokowania, okazał się elektroniczny przewodnik po programach (*electronic programme guide – EPG),* o ile jest on zintegrowany technicznie z urządzeniami kontroli rodzicielskiej; zauważono wówczas jednak, że funkcjonujące w jego ramach systemy oznakowania wywodzą się z klasyfikacji ustanowionych dla tradycyjnych form medialnych (tj. kino) i nie są dostosowywane do nowych technicznych urządzeń, co skutkowało ograniczeniem możliwości stosowania narzędzi owej kontroli. Specyfika EPG prowadzi od poziomu metainformacji do treści selekcjonowanych indywidualnie przez odbiorców i w razie dokonania określonego wyboru blokowania tych, które zostaną uznane za niepożądane (tj. zawierające przemoc czy kontekst seksualny); proponowano wprowadzenie systemu blokowania opartego o kategoryzacje odzwierciedlające perspektywę przyjmowaną przez rodziców.

43) 1.2.1. *An important distinction should be made between evaluative rating languages, with categories such as "unsuitable for children under 12 years old," and descriptive ratings languages, with categories such as "contains nudity".*

44) 1.2.2. *Considerations in allocating this responsibility include (a) who has the best information about content, (b) who has the strongest incentives to rate, and (c) who will apply rating terminology most consistently.*

Szerzej postulaty dotyczyły uzyskania większej spójności pomiędzy funkcjonującymi na konkurencyjnym, europejskim rynku systemami technicznymi i oznakowania treści (jako właściwe dla środowiska konwergentnego podano przykłady *Multimedia Home Platform*, czy NICAM[45]); zaznaczono też, aby w okresie przejściowym od system analogowego do cyfrowego, w tym do telewizji interaktywnej, utrzymać dotychczasowe, tradycyjne mechanizmy kontroli zawartości.

Internetowe systemy filtrujące bądź blokujące strony, zawierające określone słowa czy zwroty lub opierające się o ujednolicone, zakazujące albo zezwalające listy adresów internetowych (*URL*) okazały się zawodne; podobnie niepraktyczne rozwiązania, w których odpowiedzialność ponosili dostawcy treści, identyfikujący małoletnich użytkowników i blokujący im dostęp do stron zawierających niewłaściwe treści. Za najbardziej obiecujący uznano wówczas system przyjęty przez *Internet Content Rating Association* (ICRA)[46], opierający się na: 1) przyjęciu szczegółowego i opisowego języka oznakowywania treści; 2) oznaczaniu przez dostawców własnych treści, uzupełnianych listami stron trzecich, zawierającymi indywidualne oceny programowe; 3) oznakowania dokumentów w formacie HTML i odrębnych transmisji, zawierających oceny stron trzecich; 4) elastyczności wdrażania filtrów w przeglądarkach użytkowników.

Uwzględniając proces technologicznej konwergencji, zaproponowano cztery modele systemowe, przy czym najważniejszym z nich jest *Multi-Party Labeling and Rating Model System* (MPLR)*;* pozostałe potraktowano jako przydatne w okresie przejściowym[47]. Zgodnie z ogólnymi jego założeniami dostawcy treści wypełniali kwestionariusz dotyczący zawartości obejmującej: aktywność seksualną, nagość, przemoc, wulgarny język, etc.; uzyskane dane zostały przekonwertowane przez ICRA na poziom wyrazistej, opisowej informacji w formacie PICS[48] i na tej podstawie dostawca treści zamieszczał odpowiednie oznakowanie na swojej podstronie. Rodzice, korzystający z tych samych kategorii, konfigurują filtr zainstalowany w ich przeglądarkach internetowych; mogą też indywidualnie akceptować lub odrzucać strony bez oznakowania oraz uzupełniać system tzw. zielonymi lub czerwonymi listami, dostarczanymi przez strony trzecie. W ramach MPLR pierwsza warstwa opiera się na dwóch współzależnych komponentach: 1) opisie materiału i kategoryzacjach dokonywanych przez dostawcę treści oraz 2) indywidualnym opisie zawartości, których konkretny użytkownik

45) Np. NICAM, http://www.kijkwijzer.nl/index.php?id=36 [dostęp: 20.06.2012].
46) http://www.fosi.org/icra/ [dostęp: 20.06.2012].
47) 1. Multi-Party Rating System 2. Multi-Party Rating with Domestic Regulation 3. Upstream Greenlist Internet Filtering 4. Third Party Green/Redlists for Converged Content Role of Key Players.
48) Jeden z wcześniejszych systemów selekcjonowania PICS, http://www.w3.org/PICS/; późniejszy POWDER, http://www.w3.org/2007/powder/ [dostęp: 08.07.2012].

nie chce oglądać; oprogramowanie filtrujące porównuje oba opisy pod kątem kryteriów konsumenta i odpowiednio akceptuje lub blokuje określone treści. Kluczową kwestią jest tu stosowanie wspólnego, obiektywnego/neutralnego, odpowiednio precyzyjnego języka przy ustanawianiu danych kategorii, bowiem bez niego nie ma możliwości dokonywania automatycznego filtrowania zawartości; przyjmowane standardy językowe muszą być adekwatnie tłumaczone na języki państw członkowskich. Co oczywiste, kwestie te nie są łatwe do wypracowania; wysiłki zazwyczaj koncentrowane są na obrazach zawierających przemoc, seks, nagość czy wulgarny język, choć nawet przy jednolitych kryteriach trudno o jednoznaczną ocenę, jeśli choćby uwzględni się ich występowanie np. w artystycznym czy historycznym kontekście[49]. Także systemy oznaczania, opracowywane przez różnych uczestników rynku nowych technologii, muszą być balansowane i rugować słabości każdego z nich. Nacisk powinien być położony na oznakowania tworzone przez producentów treści, bowiem to oni najlepiej znają ową zawartość i oni też powszechnie docierają do użytkowników; pojawiają się tu jednak obawy niekonsekwentnego ich kategoryzowania. Natomiast dokonywanie ich przez strony trzecie mimo potencjalnej spójności i konsekwencji może powodować w praktyce omijanie większości treści, co więcej, nie mogą one uwzględniać szeroko rozumianych różnic ideologicznych, kulturowych czy innych; mogą one być przydatne przy kreowaniu wyżej wskazywanym zielonych i czerwonych list, uzupełniając tym samym oznakowania producenckie[50].

Zagadnienia klasyfikacji i oznakowania treści stanowiły też tematykę szczegółowego raportu przeprowadzonego w ramach *Safer Internet program* w 2008 roku[51], przydatnego dla rodziców i opiekunów małoletnich. Po pierwsze zatem, powinni oni poznać, wprowadzane w ramach samoregulacji lub koregulacji, systemy oznakowań zawartości. Pojęcie klasyfikacji (*clasification*) odnosi się do procesu kategoryzacji zawartości według jej odpowiedniości dla określonych grup wiekowych; oznakowanie (*labelling*) zaś do znaków (np. wizualnych lub audialnych symboli) dołączanych do filmów, rozpowszechniania telewizyjnego, na DVD, w usługach *on-line*, ujętych w schematach właściwych dla określonych typów przekazu i odmiennych co do stosowanych, dla różnych platform medialnych, me-

49) Szersze opracowanie tego zagadnienia przekracza ramy niniejszego opracowania.

50) *Third party list makers would issue redlists or greenlists covering all converged content, irrespective of delivery means. This system would require all content to have unique identifiers, like the URL for a website, transmitted directly with the content as bundled metainformation.*

51) *European Commission Information Society and Media Directorate-general Background Report on cross media rating and classification, and age verification solutions*, Safer Internet Forum, 25 – 26 September 2008, Luxembourg; por. też: D. Batorski, *Uwarunkowania i konsekwencje korzystania z technologii informacyjno – komunikacyjnych*, (w): *Diagnoza Społeczna 2007. Warunki i jakość życia Polaków*, J. Czapiński i T. Panek(red.), Vizja Press & IT, Warszawa 2007.

tod. W ramach przyjętych standardów ocenie podlegają też pojedyncze przekazy audiowizualne, tj. film, wideo gry, usługi internetowe (*rating*)[52]. Procesy klasyfikacji, kategoryzacji i ocen odzwierciedlają różnice w systemach wartości państw członkowskich, chroniących jednostki przed nieodpowiednią, naruszająca godność treścią, zawierającą zwłaszcza sceny seksu, przemocy, wulgarny lub agresywny język. Co istotne, tylko w Holandii występuje jednolity schemat klasyfikacyjny niezależny od kanałów dystrybucyjnych (*a cross media rating system*); tym większe wątpliwości powstają względem utworzenia systemu paneuropejskiego[53].

Stosowane są też kategoryzacje według wieku, zasadniczo przyjmowane w ramach samoregulacji, niekiedy zaś na podstawie twardego prawa. Są one wykorzystywane w szerokim zakresie usług *on-line*, tj. handel elektroniczny wyrobami alkoholowymi, tytoniowymi, lekami, produktami związanymi z hazardem; także przy przedstawianiu scen zawierających seks lub przemoc, czy w przypadku dostępu do sieci społecznościowych, wymagających od użytkownika przekroczenia określonej granicy wiekowej uprawniającej do korzystania z wszystkich treści legalnych (zazwyczaj chodzi o 18 lat). W przypadku zawartości *on-line* przeznaczonej wyłącznie dla osób dorosłych najczęściej stosuje się najtańszą z metod – samocertyfikację (*self certification*), polegającą na podaniu przez użytkownika informacji na temat swojego wieku, bez jakichkolwiek środków potwierdzających lub nie jej prawdziwość[54]. Również płatność *on-line* kartami (np. kredytowymi) za transakcje internetowe stanowi niepewną formę weryfikacji wieku, tym bardziej, że ich wydawcy często z założenia nie ponoszą odpowiedzialności w tej materii, przenosząc ją niejako na dostawcę

---

52) W języku polskim można – w moim przekonaniu – dla symbolicznego oznakowywania/oznaczania treści używać sformułowania 'klasyfikacja zawartości/treści', zaś do klasyfikacji według kryterium wieku – 'kategoryzacja wiekowa'; mimo że nie odpowiada to terminom przyjętym w roboczym języku, angielski zdaje się w lepszym stopniu oddawać istotę zagadnienia.

53*) A pan-European rating system refers to a system where rating and labelling schemes are the same for similar and comparable categories of content across Europe. A pan-European cross media rating system then refers to a rating and labelling regime applying a one stop rating mechanism independently of distribution platform and similar for comparable categories of content across Europe, Cross media …, op. cit.*, s. 5; *Industry and consumer organisations do not believe that a pan-European Cross Media Rating and Classification policy is either feasible, or instrumental for the protection of minors from harmful content for traditional offline media distribution platforms. Users are accustomed to existing national solutions and efforts to introduce a new system will only create confusion and not the clarity sought after by the approach, ibidem*, s. 33.

54*) Since self certification is so obviously flawed for purposes of age verification there are services using additional measures to prevent users from lying about their age. Cookies for example, which will prevent users from re-registering on a site with a different age, or walled gardens where children registering as adults to access adult content will loose access to their favourite programs from the same provider only available to minors, ibidem*, s. 18.

usług[55]. Tradycyjną i sprawdzoną, uzupełniającą formułą weryfikacyjną są analizy semantyczne, uwzględniające specyfikę językową następujących po sobie generacji i różnych środowisk. Z innych metod należy także wskazać: posługiwanie się numerem ubezpieczenia społecznego, choć ma to zazwyczaj miejsce przy transakcjach zachodzących w sektorze publicznym, czy danymi biometrycznymi, które – jak się wydaje – w niedalekiej przyszłości powinny być rozwijane i jak najszerzej stosowane.

W przypadku usług *off-line* lub nabywanych w bezpośrednim kontakcie *on-line* (np. w punktach sprzedaży urządzeń mobilnych) kontroluje się dokumenty identyfikacyjne danej osoby (dowód osobisty, paszport, prawo jazdy); w niektórych systemach krajowych do procedury weryfikacyjnej włączani są rodzice lub nauczyciele. W przypadku platform mobilnych stosuje się kombinację różnych metod; poza wymienionymi wyżej korzysta się z mechanizmów kontroli rodzicielskiej (np. zakazów subskrybowania określonych usług bez zgody rodziców, czy rozwiązań o charakterze *opt-out,* zgodnie z którymi mogą oni zastrzec dostęp do specyficznych, komercyjnych kategorii zawartości). W przypadku usług na żądanie (*video on demand*) niektórzy dostawcy wdrożyli metody kategoryzacji wiekowej jako mechanizmu kontrolnego, zapewniającego brak dostępności małoletnich do nieodpowiedniej dla nich zawartości, na podstawie jej jednostkowej oceny. Złożona sytuacja występuje w przypadku witryn społecznościowych; poza najczęściej występującą samocertyfikacją korzysta się z mechanizmów samoregulacyjnych, tj. przyjmowanie krajowych raportów dotyczących wykorzystywania dzieci jako środka powstrzymywania dorosłych od ich nagabywania; niekiedy eksperymentuje się z automatycznymi analizami semantycznymi czy jednorazowym sprawdzaniem tożsamości użytkownika.

Skuteczność wprowadzania kategoryzacji wiekowej zależy od jej uniwersalnego zaakceptowania (zwłaszcza przez powstanie szerokiego standardu dla przemysłu usług informacyjnych), bezpieczeństwa i stosunkowo niskiej kosztochłonności. Interwencje władz publicznych, głównie poprzez stanowienie wymogów prawnych, ale też np. monitorowanie obszaru muszą mieć charakter przejrzysty, być stabilne i przewidywalne oraz nie przekraczać zasady proporcjonalności; u ich podstaw stoją bowiem rozwiązania samo- i koregulacyjne, oparte o dobre praktyki i rozwój automatycznego oprogramowania kontroli rodzicielskiej w kierunku zapobiegania nieskutecznego weryfikowania prawdziwości danych doty-

55) Pewnym rozwiązaniem mogą tu być karty wydawane docelowo dla małoletnich lub mechanizmy sprawdzające przy korzystaniu przez nich z kart rodziców; podobnie *electronic Identity Cards (eID),* zawierające informacje o użytkowników na chipach, mimo iż pierwotnie wydawane w innych celach, mogą się okazać przydatne w obszarze ochrony małoletnich, *Tamże*, s. 19 – 21.

czących wieku użytkownika[56].

Zgodnie z raportami porównawczymi ukierunkowanymi na pomoc rodzicom/opiekunom w wyborze właściwych narzędzi kontroli rodzicielskiej[57] podkreślono, że urządzenia kontroli rodzicielskiej (*parental control tools*) służą prowadzeniu trzech typów działań: 1) indywidualizacja filtrowania zawartości sieci, dopuszczająca dzieci i młodzież do oglądania treści zgodnie z ustalonymi wcześniej kryteriami, według których konfigurowane jest dane narzędzie, tj. blokowanie albo wskazywanie na określoną tematykę, słowa klucze czy ujednolicone listy adresów internetowych; 2) blokowanie korzystania z danego protokołu/aplikacji niezależnie od odpowiedniości treści od małoletnich; 3) monitorowanie używania danego protokołu/aplikacji i ocena zawartości sieci pod kątem korzystania z określonych witryn internetowych.

Do badań wybrano różne aspekty obszaru, odpowiadające potrzebom rodziców/opiekunów: 1) urządzenia – komputer osobisty (PC), telefon komórkowy, konsole do gier, 2) systemy operacyjne (Windows, Mac, Linux), 3) języki, 4) typy rozwiązań (Microsoft Vista, oprogramowanie klienta, rozwiązania dostawców usług internetowych). Testowano ich: 1) funkcjonalność – posiadanie funkcji odpowiadających potrzebom rodziców, 2) efektywność – zdolność wybiórczego blokowania, 3) użyteczność – łatwość zainstalowania, konfigurowania i korzystania, 4) bezpieczeństwo – weryfikacja narzędzi zapobiegających obejściom lub wyłączeniom filtrowania przez użytkownika.

Najczęściej dostęp do Internetu (witryn, podstron czy forów społecznościowych) uzyskuje się poprzez PC. Najpowszechniejszym językiem użytkownika, w ramach którego zawiera się najszerszy zakres opcji, jest angielski; urządzenia obsługiwane w tym języku cechuje najwyższa wydajność we wszystkich w/w parametrach[58]. Wszystkie narzędzia zawierały możliwości blokowania na podstawie kryterium tematycznego, w tym łączonego z systemem czarnych/białych list, według indywidualnych, sprofilowanych preferencji użytkowników; większość umożliwia rodzicom przy-

56) Rozwiązania te muszą być oparte o zasady neutralności technologicznej i niedyskryminacji co do technologii dostępu.

57) Na podstawie: *Benchmarking of parental control tools for the online protection of children SIP-Bench II Assessment results and methodology 4 Cycle* i *Executive summary* 4 th July 2012, Safer Internet Programme oraz cykle i podsumowania poprzednich raportów 1 – 3, http://ec.europa.eu/information_society/activities/sip/projects/filter_label/sip_bench2/index_en.htm [dostęp: 20.06.2012]; por. też: Gunter, B., Rowlands, I., Nicholas, D.: *The Google Generation: Are ICT Innovations Changing Information Seeking Behaviour?* London 2009.

58) W kategorii funkcjonalności i bezpieczeństwa najwyższe oceny uzyskały różne oprogramowania; w różnych okresach badawczych: Vise, CyberSieve, Windows Vista, Kaspersky, PureSight (Owl), Profil Parental Filter, Telekom Kinderschutz Software, Norton online Family; wiele urządzeń ma możliwość blokowania MSN Messengera, ale mniej niż połowa pozwala na blokowanie Skype'a.

najmniej ramowe śledzenie historii małoletnich w Internecie, niektóre pod kątem alarmowania w przypadku odwiedzania stron zawierających np. przemoc. Najczęstszym mankamentem okazał się dostęp do zakazanych stron poprzez witryny translacyjne czy podręczną pamięć wyszukiwarek[59]. Efektywność urządzeń oceniana jest jako niska. Przede wszystkim udział zawartości niefiltrowanej jest znaczący, choć treści oznakowywane jako przeznaczone wyłącznie dla osób dorosłych są lepiej weryfikowane niż inne kategorie, tj. samoagresja, rasizm czy przemoc; skuteczność jest niższa dla zawartości, tj. blogi czy media społecznościowe (Web 2.0). Co do użyteczności uznanie zyskały niektóre programy[60]. Kluczowym problemem jest jednak to, że urządzenia łatwe do zainstalowania i skonfigurowania dysponują stosunkowo niewielką ofertą zabezpieczeń, względem tych, których obsługa wymaga większych umiejętności.

W przypadku dzieci dostęp do usług *on-line* (*video streaming* i komunikatorów[61]) następuje najczęściej poprzez telefony komórkowe (w tym posiadające szersze 'funkcjonalności' *smart phones)*[62]. Zauważono, że niewiele narzędzi ma zdolność do kompleksowego filtrowania stron internetowych, ograniczając się np. do poczty, SMS-ów, etc. Skuteczność filtrowania zawartości, mimo że według jej charakterystyki wykazuje zbieżność ukierunkowań ze środowiskiem PC, jest mniejsza (ale różnice niwelują się), natomiast większość urządzeń, w podstawowych zakresach zabezpieczania, instaluje się automatycznie, choć ich działanie i obsługa nie są w pełni zrozumiałe dla użytkownika. Fakt, że większość małoletnich traktuje swoje telefony komórkowe jako indywidualną własność, nie znajduje odzwierciedlenia w funkcjonalności narzędzi kontroli rodzicielskiej; dla przykładu opiekunowie, aby monitorować działalność swoich dzieci, w zasadzie muszą wziąć od nich telefon, sprawdzić raporty, etc. – celowe jest zatem wprowadzanie i stosowanie aplikacji równoległych dla telefonu dziecka i rodzica[63].

Konsole do gier są urządzeniami w skali masowej zapewniającymi dostęp do Internetu, w celu grania, czatowania z innymi uczestnikami lub przesyłania treści czy dokonywania zakupów produktów. Mimo iż wyposażone są w narzędzia filtrujące, to nie weryfikują one podstron internetowych według kryterium zawartości; niekiedy można wykorzystywać do nich urządzenia zewnętrzne (*Astaro, Trend Micro Kids Safety*). Obserwuje się,

59) Dla przykładu podaje się tzw. *Google cache,* stanowiące usługę polegającą na kopiowaniu witryn internetowych i przetrzymywaniu ich zawartości na serwerach własnych w celu jej dostarczenia, w przypadku niefunkcjonowania strony oryginalnej, za: http:/www.googleguide.com/cached_pages_html [dostęp: 28.06.2012].

60) Np. *CyberPatrol, Kaspersky i Open DNS -1.*

61*) by using specific applications such as Instant Messaging* (narzędzie typu gadu-gadu).

62) Badano *Safe Eyes (Iphone)* i *Security Shield (BlackBerry, Symbian, Windows Mobile, Android)*.

63) Na razie stwierdzono, że aplikację taką ma jedno urządzenie.

podobne jak w poprzednich grupach, kierunki weryfikacji treści i mniejszą względem PC efektywność; co więcej, są one mniej znane rodzicom[64].

Reasumując

Analiza ponad dwudziestoletniego okresu kształtowania się polityki Unii Europejskiej odnośnie ochrony dzieci i młodzieży w sektorze nowych technologii komunikacyjnych nasuwa wnioski ogólniejszej natury.

Należy przyjąć założenie, że współczesne środowisko „konwergencyjne" stawia współczesnym organizacjom międzynarodowym, państwom czy szerzej społeczeństwom poważne wyzwania; w szczególności obserwuje się to w zakresie ochrony małoletnich przed negatywną zawartością, zarówno tą nielegalną, jak i zgodną z prawem, ale nieodpowiednią dla dzieci i młodzieży. Podstawowym problemem, jaki pojawił się w związku z rozwojem usług *on-line*, jest to, że w praktyce efektywne sprawowanie nad nimi jurysdykcji krajowej budzi poważne wątpliwości, a tym samym zwalczanie niepożądanych zjawisk czy egzekwowanie określonych standardów jest co najmniej znacząco utrudnione[65]; w zasadzie wymaga międzynarodowego, a przynajmniej ponadnarodowego podejścia, a to z wielorakich przyczyn jest na obecnym etapie w zasadzie niewykonalne. Tym bardziej odpowiedzialność spoczywa na użytkownikach końcowych, tj. sami małoletni czy sprawujący nad nimi kontrolę rodzice/opiekunowie lub nauczyciele, którzy dla jej właściwej realizacji muszą dostatecznie poznać i zrozumieć środowisko nowych technologii. Jest to szczególnie trudne wyzwanie; z jednej strony bowiem wynika ono z szerokiego zakresu zagadnień, ich złożoności i zróżnicowania problematyki (także z uwagi na wielopoziomowość jej regulacji); ten aspekt ma charakter indywidualny[66].

W raporcie z 2008 roku poświęconym bezpieczniejszemu używaniu przez dzieci z UE Internetu w sposób przejrzysty pokazano perspektywę rodzi-

64) *Game consoles were not tested under the fourth cycle. This is due to the fact that no new filter appeared on the market at that time* (4).

65) Szerzej na temat jurysdykcji por. np. P. Milik, *Komplementarność jurysdykcji Międzynarodowego Trybunału Karnego i trybunałów hybrydowych, wyd.* Elipsa, Warszawa 2012, zwłaszcza rozdział 2; E. Murawska-Najmiec, *Informacja na temat działań społeczności międzynarodowej na rzecz objęcia Internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji*, analiza biura KRRiT Nr 7/2005, http://www.krrit.gov.pl/Data/Files/_public/pliki/publikacje/analiza2005_07.pdf [dostęp: 10.06.2012].

66) W skali ogólnej pojawia się tu natomiast problem wykluczenia społecznego, będącego zwłaszcza skutkiem ubóstwa, które może prowadzić w efekcie do tzw. dziedziczenia analfabetyzmu w tym obszarze, por. np. http://ec.europa.eu/employment_social/2010againstpoverty/index_nl.htm; szersze omówienie tego zagadnienia wymaga odrębnego opracowania, por. np. G. Hołowiński, *Problem wykluczenia cyfrowego w Polsce. Technologia informacyjna i komunikacyjna – zagrożeniem czy szansą?* [w:] Szewczyk A. (red.), *Komputer – przyjaciel czy wróg?*, Wydawnictwo Uniwersytetu Szczecińskiego, Szczecin 2005 .

cielską[67]; badanie ukierunkowane zostało na ustalenie, jak opiekunowie postrzegają tę problematykę, jakie przyjmują strategie w kontrolowaniu dzieci od 6 do 17 roku życia i jaka jest ich świadomość co do środków bezpieczeństwa.

W szczególności ustalono, że średnio dla 27 krajów UE 75% rodziców sądzi, że ich dzieci korzystają z Internetu (także przy pomocy mobilnych technologii), przy czym przekonanie to różni się znacząco w poszczególnych krajach (najmniej we Włoszech – 45%, najwięcej w Finlandii – 91%); niewątpliwe jest natomiast to, że proces ten systematycznie się rozszerza. Dzieci najczęściej używają go w domu lub szkole; w wieku do 10 lat zazwyczaj dzielą PC z innymi domownikami, starsi mają własny komputer lub korzystają z niego poza miejscem zamieszkania (np. w kafejkach internetowych)[68].

Opiekunowie najbardziej obawiają się, że małoletni narażeni są na styczność z obrazami przemocy lub seksu (45%), kontakty ukierunkowane na seksualne wykorzystanie (*grooming* – 46%), nękanie przez rówieśników, otrzymywanie informacji o samoagresji (w tym samobójstwach), zaburzeniach żywienia (anoreksja); niepokojące jest również to, że mogą przekazywać dane osobowe i inne wrażliwe informacje. Tylko niespełna 1/3 dzieci prosi o pomoc w przypadku pojawienia się problemów związanych z korzystaniem z Internetu, tj. nękanie, podejrzany kontakt z obcą osobą, ale też z obrazami agresji czy seksu, przy czym najwięcej w Danii (48%), najmniej zaś w Wielkiej Brytanii (15%)[69].

W sytuacjach, kiedy dzieci korzystają z Internetu w domu, rodzice bardzo często (w tym zawsze) rozmawiają z nimi o zagrożeniach w Internecie, pytają, czym się zajmują w Internecie, etc. (74%), znajdują się niedaleko dzieci, podczas gdy są one *on-line* (61%, ale towarzyszy im tylko 36%), lub sprawdzają: historię ich aktywności (44%), czy mają one profile na portalach społecznościowych (30%) oraz kontrolują ich prywatną korespondencję (24%)[70].

67) *Towards a safer use of the Internet for children in the EU – a parents' perspective Analytical report Fieldwork*; *Towards a safer use of the Internet for children in the EU – a parents' perspective Summary Fieldwork*: October 2008 Publication: December 2008 http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf;http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2008.pdf, [dostęp: 29.06.2012]; *Earlier surveys on this topic were carried out in 2003/04* (*Special Eurobarometer No 203* and *Candidate countries Eurobarometer CC-EB 2004.1*) and *2005/06 (Special Eurobarometer No 250*).

68*) Almost two-thirds of the respondents said that their child had a mobile phone and only 37% said the opposite. Of the children with a mobile phone, the largest group had one without access to the Internet (50%), while 11% had a mobile phone with such access, and 3% of the parents did not know if this was the case,* Ibidem s. 7.

69) Por. też: *EU Kids online. Comparing children's online opportunities and risks across Europe. European Research in Cultural, Contextual and Risk Issues in Children's Safe Use of the Internet and New Media (2006-2009)*. Dokument elektroniczny dostępny online: http://eprints.lse.ac.uk/21656/1/D3.2_Report- Cross_national_comparisons.pdf [dostęp: 3.01.2012].

70) *Parents who were Internet users themselves said they operated more control over their child's*

Używanie monitorującego lub filtrującego oprogramowania zadeklarowało średnio 59% badanych; rozbieżność była jednak znaczna, najwięcej, bo aż 85% zanotowano w Wielkiej Brytanii, natomiast najmniej w Rumunii – 21%. Większość niekorzystających z zabezpieczeń twierdziła, że ufa swoim dzieciom (64%) lub nie wie, jak używać narzędzi (14%). W przypadku nielegalnej lub szkodliwej treści zaobserwowanej w Internecie aż 92% myśli o poinformowaniu Policji, 38% tzw. gorących linii a 33% organizacji pozarządowych; średnio 38% czyni to[71].

Opiekunowie nakładają na małoletnich przede wszystkim następujące ograniczenia w korzystaniu z Internetu: przekazywanie prywatnych informacji (92%), zakupy *on-line* (84%), rozmowy z nieznajomymi (83%), długie spędzanie czasu *on-line* (79%) oraz zakładanie profilu na portalu społecznościowym (63%) i korzystanie z tzw. *chat rooms* (61%).

Rodzice uważają, że poprawić bezpieczeństwo w Internecie może: odpowiednie nauczanie w ramach programów szkolnych (88%), kampanie informacyjne o ryzyku w sieci czy informacje na witrynach internetowych używanych przez dzieci (87%), surowe regulacje dla przemysłu produkującego zawartość i usługi *on-line* (86%), poradnicze punkty kontaktowe (84%), usprawnienie oprogramowania monitorującego (80%), szkolenia organizowanie dla rodziców przez organizacje pozarządowe czy władze publiczne (70%). Informacje na temat bezpieczeństwa w Internecie opiekunowie czerpią od znajomych (71%), z mediów (62%), witryn internetowych (39%), dostawców usług internetowych (36%).

W przypadku Polski obserwuje się zjawisko częstszego niż średnia europejska łączenia się małoletnich z Internetem poza możliwościami kontroli rodzicielskiej, za pomocą komputera osobistego (PC), będącego w ich prywatnej dyspozycji (i umieszczonego w miejscu zamieszkania), lub przez urządzenia mobilne, tj. telefon komórkowy czy w ostatnim okresie *smart phone, iPhone.* Niepokojącą konkluzją z ostatnich badań jest stwierdzenie, że w Polsce monitorowanie przez osoby dorosłe używania Internetu przez dzieci jest mniejsze niż przeciętne w innych krajach europejskich, co prawdopodobnie łączy się zarówno z faktem, iż w polskich rodzinach to małoletni częściej korzystają z nowych technologii niż ich opiekunowie, przez co PC umieszczany jest w ich własnym

use of the Internet – this was as expected, since most strategies for parental supervision assume that parents know how to use the Internet, e.g. how to check their child's Internet history.
Parents with a lower level of educational attainment were slightly more likely to check their child's online activities. For example, one-third of the least-educated parents said they regularly checked the messages in their child's e-mail or IM account compared to only slightly more than one-fifth of parents in the highest educational category, Tamże, s. 12.

71*) Parents who did not use the Internet were more likely not to know how they would report illegal or harmful content seen on the Internet. For example, almost one-fifth of the parents who did not use the Internet did not know they could report illegal content to a hotline set up for this purpose compared to 12% of the parents who did use the Internet, Tamże*, s. 15.

pokoju lub wydzielonej części pomieszczenia, jak i z mniejszą kompetencją medialną rodziców czy nauczycieli; rodziny i środowiska szkolne powinny więc uczyć się, jak radzić sobie z zagrożeniami sieci, a dorośli ponadto jak skutecznie kontrolować aktywność dzieci w tym obszarze[72].

Dlatego z perspektywy rodziców szczególne znaczenie ma znajomość: 1) rodzajów i charakteru zagrożeń, właściwych dla środowiska *on-line* – zwłaszcza jeśli chodzi o nowe zjawiska, tj. *grooming* czy *cyber-bullying*; 2) systemów oznakowania treści i kategoryzacji wiekowych oraz 3) technicznych aspektów dostępu do usług informacyjnych i zabezpieczeń przed nieuprawnionym do nich dostępem.

Jednostkowa realizacja powyższych wyzwań nie doprowadzi jednak do uzyskania oczekiwanych efektów w skali ogólnej. Niewątpliwie kluczową rolę odgrywają tutaj państwa członkowskie, które pod auspicjami UE powinny doprowadzić do większej spójności systemów klasyfikacji wiekowej i treści, a przede wszystkim do uszczegółowienia standardów, w ramach których ma następować ich wykonywanie na poziomie krajowym[73]. Powinny też kształtować warunki sprzyjające permanentnej edukacji obywatelskiej w tym obszarze, traktując przyjmowane inicjatywy jako element bezpieczeństwa społecznego[74].

Jeśli chodzi o kwestie poznania zagrożeń i systemów klasyfikacji, kategoryzacji czy oznaczania zawartości usług *on-line*, to fundamentalne znaczenie ma tutaj spójna, informacyjna polityka krajowa, ukierunkowana na udostępnienie społeczeństwom państw członkowskich kompleksowej, szeroko rozpowszechnianej wiedzy w tym zakresie, zwłaszcza o progra-

72) *Sugeruje to konieczność lepszej edukacji polskich dzieci odnośnie tego, jak sobie radzić z internetowymi zagrożeniami, a na polskich rodziców nakłada obowiązek monitorowania, jak ich dzieci korzystają z Internetu,* L. Kirwil, (2011). *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo - część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców*. Warszawa: SWPS – EU Kids Online – PL, s. 11.

73) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions European Strategy for a Better Internet for Children,* Brussels, 4.5.2012 COM(2012) 203 final.

74) Szersze rozważenie tego zagadnienia przekracza ramy niniejszego opracowania; por. np. K. Badźmirowska – Masłowska, *Ochrona dzieci i młodzieży w systemie mediów audiowizualnych w Polsce z perspektywy rozwiązań europejskich,* Archiwum Kryminologii, XXIX – XXX, 2007 – 2008; M. Borkowska, E. Murawska-Najmiec. P. Stępka, A. Woźniak, *Organizacje międzynarodowe i wybrane państwa europejskie wobec edukacji medialnej,* Analiza Biura KRRiT 2/2010, Warszawa 2010; *Cyfrowa Przyszłość. Edukacja medialna i informacyjna w Polsce– raport otwarcia,* Fundacja Nowoczesna Polska na rzecz Narodowego Instytutu Audiowizualnego, Warszawa 2012; *Handbook of children and media,* D. G Singer i J. L. Singer (ed.), Thousand Oaks, London, Delhi: Sage Publications, Inc., 2001; *Media Literacy Profile, EUROPE,* http://ec.europa.eu/culture/media/literacy/docs/studies/country/europe.pdf (29.06.2012).
Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European approach to media literacy in the digital environment, Brussels, 20.12.2007 COM(2007) 833 final.

mach, projektach czy badaniach prowadzonych na poziomie europejskim. Powinno to następować we współpracy z zainteresowanymi stronami, reprezentującymi zwłaszcza odnośny przemysł i organizacje pozarządowe, które niekiedy pełnią istotne funkcje w krajowej realizacji powyższych programów czy projektów. W gestii władz publicznych pozostaje przyjęcie określonych strategii, obejmujących przede wszystkim inicjatywy kampanii informacyjnych, prowadzonych przez różne podmioty sektora publicznego czy prywatnego. Jak się wydaje w obecnej sytuacji, w Polsce polityka taka nie funkcjonuje systemowo, bowiem docierające do społeczeństwa informacje mają charakter sporadyczny i fragmentaryczny; może to wynikać z faktu niedostatecznego rozumienia powagi i skali zagrożeń, występujących w środowisku *on-line* dla bezpieczeństwa młodego pokolenia.

Szczególnym praktycznym wyzwaniem dla rodziców i nauczycieli są niewątpliwie trudne do nauczenia kwestie techniczne; nie wszyscy opiekunowie orientują się choćby w kwestiach funkcjonowania zabezpieczeń systemów operacyjnych (tj. *Windows*)[75], filtrowania stron internetowych, także pod kątem ocen gier internetowych, limitowania czasu spędzanego przy komputerze, czy – z drugiej strony – mają wystarczającą wiedzę i umiejętności dotarcia do instytucji świadczących usługi poradnicze, czy prawne w związku z nielegalną lub szkodliwą treścią *on-line*[76].

Zakończenie

Ta kluczowa kwestia łączy się z głównym obszarem problemów, wynikających z uwarunkowanych technicznie, transgraniczności usług *on-line* i dynamicznego ich rozwoju. Nie dość, że nie jest łatwo o porozumienie w zakresie wypracowania wspólnych standardów ochrony małoletnich nie tylko na poziomie międzynarodowym (uniwersalnym czy regionalnym), ale nawet w ramach Unii Europejskiej, to – jak już wskazywano powyżej – szeroko rozumiane trudności jurysdykcyjne powodują praktycznie niedostateczną skuteczność egzekucji nawet już przyjętych regulacji czy standardów etycznych. W takiej sytuacji celowym wydaje się rozważenie roli, jaką mogliby odgrywać czołowi, działający w skali międzynarodowej przedstawiciele przemysłów nowych technologii. Chodzi tu o takich potentatów *know - how* jak *Google* (wyszukiwarka), którzy jednak – co oczywiste – musieliby działać na zasadach dobrowolności i w ścisłym ze sobą porozumieniu, przy

75) Np. czy filtr wbudowany jest automatycznie, czy należy go zainstalować samemu i jak można go zamówić u swojego dostawcy Internetu, wreszcie jaki jest schemat i zakres jego działania i czy i na jakich podstawach można dokonywać wyboru; czy są one płatne, czy darmowe, etc.

76) Por. np. fundację 'Dzieci niczyje' i NASK świadczące usługi w ramach punktu kontaktowego programu (dyżurnet.pl) czy typu *help line,* (helpline.org.pl) http://www.saferinternet.pl/safer_internet_w_polsce.html.

czym nawet jeśli oparte byłoby ono o ogólne regulacje międzynarodowe (w rodzaju karty praw dzieci w środowisku *on-line*), powinno mieć charakter *soft law* i być uzupełniane bardziej szczegółowymi postanowieniami wynikającymi np. z kodeksów dobrych praktyk. W jego ramach można byłoby się oprzeć o następujący quasisylogizm: 1) zaangażowane podmioty stosują wspólne kryteria oceny treści, warunkujące uznanie niektórych z nich za nielegalne lub co najmniej szkodliwe dla określonych kategorii wiekowych użytkowników – jest to już realizowane w zakresie seksualnego wykorzystywania dzieci i pornografii dziecięcej, etc., a może zostać rozszerzone do kwestii handlu dziećmi; 2) przy zakładaniu kont, np. w *Google,* osobom poniżej 18 roku życia muszą brać udział ich rodzice/opiekunowie, ustalający poziom ochrony w zależności od wieku – tu istotna jest skuteczność weryfikowania dorosłych uczestników procesu, poprzez np. wzmocnienie współpracy z: dostawcami treści, technologii, bankami przy sprawdzaniu różnego rodzaju kart. Jak się wydaje, w przyszłości będzie można korzystać także z analizy danych biometrycznych. Powyższe założenia stoją u podstawy dokonywania ocen przez *Google,* która jednak nie poprzestaje na ostrzeżeniach, kierowanych do rodziców, ale w ramach szczególnego nadzoru nad tymi kontami automatycznie releguje treści nieodpowiednie dla wieku użytkownika danego konta, według indywidualnych ustaleń z dorosłymi opiekunami małoletnich, przekazując im także emaile, wskazujące na historię konta i uwypuklające ewentualną, nieusuniętą przez system potencjalnie szkodliwą zawartość[77].

Przedstawione powyżej wnioski, dotyczące głównych aspektów ochrony dzieci i młodzieży przed współczesnymi zagrożeniami środowiska *on-line* są oczywiście tylko próbą wskazania ewentualnych możliwych kierunków rozwiązań; niemniej jednak, uwzględniając choćby powszechną dostępność do stron o charakterze pedofilskim[78], wszelkie rozważania i poszukiwania praktycznie efektywnych rozwiązań w zapewnianiu bezpieczeństwa dzieci w obszarze nowych technologii wydają się przydatne.

77) Narzędzia mogą być stosowane analogicznie do współcześnie używanych już w obszarze wyświetlania reklamy (analizy treści strony i zachowań użytkowników).

78) Por. np. TOR (The Onion Route), projekt polegający na kierowaniu ruchu internetowego przez sieć użytkowników (wolontariuszy) od komputera klienta do serwera, co praktycznie uniemożliwia fizyczne zlokalizowanie komputera klienta,
https://www.torproject.org/index.html.en, Tor (The Onion Route)
https://www.torproject.org/eff/tor-legal-faq.html.en; http://en.wikipedia.org/wiki/Tor_ (anonymity_network) [dostęp: 08.07.2012].

Bibliografia

Druki zwarte:

Batorski D., *Uwarunkowania i konsekwencje korzystania z technologii informacyjno – komunikacyjnych*, [w:] Czapiński J. i Panek T. (red.), *Diagnoza Społeczna 2007. Warunki i jakość życia Polaków*, Vizja Press & IT, Warszawa 2007.

Cellary W. (red.), *Przemiany społeczne*, [w:] *Polska w drodze do globalnego społeczeństwa informacyjnego. Raport o rozwoju społecznym*, Wyd. UNDP, Warszawa 2002.

Chałubińska–Jentkiewicz K., *Media audiowizualne. Konflikt regulacyjny w dobie cyfryzacji*, Wolters Kluwer Polska, Warszawa 2011.

Dijk, J. van: *Społeczne aspekty nowych mediów. Analiza społeczeństwa sieci.* Warszawa 2010.

Goggin G., *Cell Phone Culture: Mobile Technology in Everyday Life*, Londyn 2006.

Gorman L., McLean D., *Media i społeczeństwo. Wprowadzenie historyczne*, WAiP, Kraków 2010.

Gunter, B., Rowlands, I., Nicholas, D., *The Google Generation: Are ICT Innovations Changing Information Seeking Behaviour?* London 2009.

Handbook of children and media, D. G Singer i J. L. Singer (ed.), Thousand Oaks, London, Delhi: Sage Publications, Inc., 2001.

Hołowiński G., *Problem wykluczenia cyfrowego w Polsce. Technologia informacyjna i komunikacyjna – zagrożeniem czy szansą?* [w:] Szewczyk A. (red.), *Komputer – przyjaciel czy wróg?*, Wydawnictwo Uniwersytetu Szczecińskiego, Szczecin 2005.

Jenkins H., *Kultura konwergencji, zderzenie starych i nowych mediów*, WAiP, Warszawa 2007.

Sierocki R., Sokołowski M., *Metafory sieci. (Re)definiowanie Internetu*, [w:] Jeziński M. (red.), *Nowe media w systemie komunikowania: Edukacja, cyfryzacja*, Wyd. A. Marszałek, Toruń 2011.

Sitek M., *Prawne i instytucjonalne ramy zwalczania handlu ludźmi,* [w:] Sitek B., Dammacco G. i in. (red.), *Wykorzystywanie człowieka w XX i XXI wieku*, UWM Wydział Prawa i Administracji, Olsztyn 2012, s. 331-344.

Czasopisma:

Badźmirowska – Masłowska K., *Ochrona dzieci i młodzieży w systemie mediów audiowizualnych w Polsce z perspektywy rozwiązań europejskich,* Archiwum Kryminologii, XXIX – XXX, 2007 – 2008.

Gruchoła M., *Ochrona małoletnich internautów w prawie i praktyce Unii Europejskiej,* Rozprawy Społeczne, nr 1 (V) 2011.

Wyrozumska A., *Znaczenie prawne zmiany statusu Karty Praw Podstawowych Unii Europejskiej w Traktacie Lizbońskim oraz Protokołu Polsko-Brytyjskiego*, Przegląd Sejmowy 2008 Nr 2(85).

Dokumenty (*hard law*/ *soft law*):

Commission Communication on the Study on Parental Control of Television Broadcasting (1999), Brussels, 19/07/99 COM/99/371 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions A European approach to media literacy in the digital environment, Brussels, 20.12.2007 COM(2007) 833 final.

The Commission Communication 'i2010 — A European Information Society for growth and employment' COM(2005)0229*).*

Communication from the Commission to the European Parliament, the council, the European Economic and Social Committee and the Committee of the Regions a digital agenda for europe COM (2010) 245 final/2 *; European Parliament resolution of 5 May 2010 on a new Digital Agenda for Europe:* 2015.eu (2009/2225(INI)); *Council conclusions of 31 May 2010 on digital agenda in Europe*, COM/2010/0245 final.

Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, European strategy for a better internet for children, COM (2012) 196 final; *Decision No 276/1999/EC of the European Parliament and of the Council of 25 January 1999 adopting a Multiannual Community Action Plan on promoting safer use of the Internet and new online technologies by combating illegal and harmful content primarily in the area of the protection of children and minors, (the Safer Internet Action Plan 1998-2004); Decision No 854/2005/EC of the European Parliament and of the Council of 11 May 2005 establishing a multiannual Community Programme on promoting safer use of the Internet and new online technologies (the Safer Internet plus programme 2005-2008); Decision No 1351/2008/EC of the European Parliament and of the Council of 16 December 2008 establishing a multiannual Community programme on protecting children using the Internet and other communication technologies*, OJ. EU. L. 348/118, 24.12.2008.

Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce) O. J. L 178 , 17/07/2000 P. 0001 – 0016.

Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) (codified version) *O. J.L 095 , 15/04/2010 P. 0001 – 0024.*

European Framework for Safer Mobile Use by Younger Teenagers and Children SIPMC 07/2; za: http://ec.europa.eu/information_society/activities/sip/self_reg/phones/index_en.htm; http://www.gsma.com/publicpolicy/wp-content/uploads/2012/03/Safer_Mobile_Flyer-1.pdf; 2010 Implementation report of the European Framework; 2009 Implementation Report of the European Framework, etc. http://www.gsma.com/gsmaeurope/safer-mobile-use/european-framework.

Green Paper on the Protection of Minors and Human Dignity in Audiovisual and Information Services, COM (96) 483 final, 16 October 1996.

Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, O.J. L 378.

Kodeks karny z 6 czerwca 1997, Dz. U, 1997 nr 88, poz. 533, z późniejszymi zamianami.

Council Recommendation 98/560/EC of 24 September 1998 *on the development of the competitiveness of the European audiovisual and information services industry by promoting national frameworks aimed at achieving a comparable and effective level of protection of minors and human dignity*, O. J. L 270 of 7.10.1998.

Recommendation of the European Parliament and of the Council of 20 December 2006 on the protection of minors and human dignity and on the right of reply in relation to the competitiveness of the European audiovisual and on-line information services industry, O.J. L 378.

Resolution of the council and of the representatives of the governments of the member states, meeting within the council of 17 February 1997 on illegal and harmful content on the internet, 97/C 70/01.

1t. *Council Resolution, of 1 March 2002 on the protection of consumers, in particular young people, through the labelling of certain video games and computer games according to age group* OJ. EC, C65, 14.3.2002, p.2.

Dokumenty (raporty i analizy):

Background report on age verification, cross media rating and calisfication and age veryfication solutions (2008), Safer Internet Forum 25 – 26 September 2008: http://ec.europa.eu/information_society/activities/sip/docs/pub_consult_age_rating_sns/reportageverification.pdf.

Benchmarking of parental control tools for the online protection of children SIP-Bench II Assessment results and methodology 4 Cycle i *Executive summary* 4 th July 2012, Safer Internet Programme oraz cykle i podsumowania poprzednich raportów 1 – 3, http://ec.europa.eu/information_society/activities/sip/projects/filter_label/sip_bench2/index_en.html;http://ec.europa.eu/employment_social/2010againstpoverty/index_nl.htm.

Borkowska M., E. Murawska-Najmiec E., Stępka P., Woźniak A., *Organizacje międzynarodowe i wybrane państwa europejskie wobec edukacji medialnej,* Analiza Biura KRRiT 2/2010, Warszawa 2010.

Cyfrowa Przyszłość. Edukacja medialna i informacyjna w Polsce– raport otwarcia, Fundacja Nowoczesna Polska na rzecz Narodowego Instytutu Audiowizualnego, Warszawa 2012.

DVB Parental Control Report October 2000 *Annex B to 001213_DT5634 Parental Control in a Converged Communications Environment Self-Regulation, Technical Devices, and Meta-Information*.

Evaluation Report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 on protection of minors and human dignity, COM(2001) 106final - 27.02.2001*; Second evaluation report from the Commission to the Council and the European Parliament on the application of Council Recommendation of 24 September 1998 concerning the protection of minors and human dignity",* COM/2003/0776 final.

EU Kids online. Comparing children's online opportunities and risks across Europe. European Research in Cultural, Contextual and Risk Issues in Children's Safe Use of the Internet and New Media (2006-2009): http://eprints.lse.ac.uk/21656/1/D3.2_Report- Cross_national_comparisons.pdf.

Kirwil L., (2011). *Polskie dzieci w Internecie. Zagrożenia i bezpieczeństwo - część 2. Częściowy raport z badań EU Kids Online II przeprowadzonych wśród dzieci w wieku 9-16 lat i ich rodziców*. Warszawa: SWPS – EU Kids Online – PL.

Media Literacy Profile, EUROPE, http://ec.europa.eu/culture/media/literacy/docs/studies/country/europe.pdf.

Murawska-Najmiec E., *Informacja na temat działań społeczności międzynarodowej na rzecz objęcia Internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji*, analiza biura KRRiT Nr 7/2005, http://www.krrit.gov.pl/Data/Files/_public/pliki/publikacje/analiza2005_07.pdf.

Report of 16 February 2009, of European Parliament on the protection of consumers, in particular minors, in respect of the use of video games, 2008/2173(INI), Committee on the Internal Market and Consumer Protection.

Towards a safer use of the Internet for children in the EU – a parents' perspective Analytical report Fieldwork; *Towards a safer use of the Internet for children in the EU – a parents' perspective Summary Fieldwork*: October 2008 Publication: December 2008 http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/analyticalreport_2008.pdf;http://ec.europa.eu/information_society/activities/sip/docs/eurobarometer/eurobarometer_2008.pdf; *Earlier surveys on this topic were carried out in 2003/04* (*Special Eurobarometer No 203* and *Candidate countries Eurobarometer CC-EB 2004.1*) and *2005/06 (Special Eurobarometer No 250*).

Netografia:

http://ec.europa.eu/culture/media/literacy/index_en.htm.
http://ec.europa.eu/information_society/apps/projects/factsheet/index.cfm?project_ref=SIP-2006-UE-211001.
http://ec.europa.eu/information_society/activities/sip/events/forum/index_en.htm.
http://ec.europa.eu/information_society/activities/sip/projects/centres/panels/index_en.htm.
http://ec.europa.eu/information_society/activities/sip/projects/completed/illeg_content/index_en.htm.
http://ec.europa.eu/justice/fundamental-rights/rights-child/european-forum/index_en.htm.
http://www.fosi.org/icra.
http://www.kijkwijzer.nl/index.php?id=36.
http://www.pegi.info/en/index/id/33, http://www.pegionline.eu/pl/index.
http://www.saferinternet.org/web/guest/safer-internet-day.
http://www.saferinternet.pl/safer_internet_w_polsce.html.
http://www.helpline.org.pl
http://dyzurnet.pl/zglos_nielegalne_tresci_ref.php.
https://www.torproject.org/eff/tor-legal-faq.html.en.
https://www.torproject.org/index.html.en.
http://en.wikipedia.org/wiki/Tor_(anonymity_network).
http://www2.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20Online%20reports.aspx.
http://www.w3.org/2007/powder.