Biuro Krajowej Rady Radiofonii i Telewizji

Departament Strategii i Analiz

KRAJOWA RADA RADIOFONII I TELEWIZJI

Informacja na temat działań społeczności międzynarodowej na rzecz objęcia Internetu systemem prawa przy jednoczesnej ochronie swobody wypowiedzi i informacji

Ewa Murawska-Najmiec

Grudzień 2005

ANALIZA BIURA KRRiT

a)

Nr 7/2005

1. WSTĘP

Internet a swoboda wypowiedzi i informacji

Internet to niezwykle dynamicznie rozwijające się medium, w którym swoboda wypowiedzi i przepływu informacji przejawia się w najbardziej spektakularny sposób. W powszechnym odbiorze stanowi on „ostatnią oazę wolności", a postrzeganiu temu sprzyja jego transnarodowy, globalny charakter oraz występujące w nim nowe wzory komunikowania.

Swoboda wypowiedzi i informacji stanowi jedno z podstawowych praw człowieka - standard obowiązujący w państwach demokratycznych. Źródłem jest art. 10 Europejskiej Konwencji Praw Człowieka, a podobne sformułowania można znaleźć także w art. XIX Powszechnej Deklaracji Praw Człowieka, art. XIX Międzynarodowego Paktu Praw Obywatelskich i Politycznych czy art. 11 Karty Praw Podstawowych Unii Europejskiej. Przyjmuje się, że nowe technologie, w tym Internet, nadają temu prawu człowieka nowy wymiar, znacznie zwiększając możliwości korzystania z niego [1].

Jednocześnie jednak toczy się bardzo ożywiona debata w poszczególnych krajach i na forum międzynarodowym na temat relacji między Internetem i systemem prawa (nie ma wątpliwości, zgodnie ze znanym powiedzeniem, że „to, co jest nielegalne *off-line* jest równie nielegalne *online"* – pytanie tylko, jak wyegzekwować przestrzeganie prawa w Internecie) oraz na temat zarządzania Internetem jako systemem komunikacji jak również ewentualnego zakresu i metod regulacji zawartości przekazywanej przez Internet.

Zadaniem niniejszego opracowania jest wstępne przybliżenie przebiegu i charakteru powyższej debaty oraz działań podejmowanych w tym zakresie. Nie pretenduje ono oczywiście do wyczerpania tematu, a jedynie do podania przykładów różnych podejść i działań zgodnie z nimi podejmowanych. Ma ono na celu wniesienie pewnego zasobu informacji i rozmaitych przykładów sposobów podejścia do Internetu do toczącej się także w Polsce debaty na temat dopuszczalnych granic swobody w Internecie oraz metod przeciwdziałania naruszeniom tej swobody, a także zapewnienia bezpiecznego korzystania z Internetu. Przedmiotem niniejszego opracowanie jest bowiem relacja prawo – Internet w odniesieniu do internetowej zawartości *(content)*. Tym samym nie dotyczy ono licznych innych dziedzin polityki publicznej w zakresie Internetu (patrz Tabela nr 1). Jest ono natomiast elementem szerszej dyskusji o mediach elektronicznych i zmieniającego się porządku regulacyjnego, którym są objęte.

---

[1] Por. Karol Jakubowicz, "Human Rights and the Information Society: A preliminary Overview" Preparatory Group on Human Rights, the Rule of Law and the Information Society IP1(2004)47. Strasbourg, Council of Europe, 7 September 2004, http://www.unesco.nl/images/jakubowicz_working_paper.pdf. Por. Declaration of the Committee of Ministers on human rights and the rule of law in the Information Society CM(2005)56 final. Strasbourg: Council of Europe, 13 May 2005.

b) **Internet jako rozwijające się medium elektroniczne**

Internet tworzy nowe wzory komunikowania, uzupełniając komunikację porozumiewawczą „*jeden do jednego*" (z punktu do punktu, za pośrednictwem środków łączności), czyli prywatną, nie podlegającą regulacji ze względu na zawartość, oraz tradycyjną radiodyfuzję „*jeden do wielu"* (komunikację publiczną, a więc regulowaną) - komunikacją grupową, interaktywną *„wszyscy ze wszystkimi*", a także nielinearną, w której to uczestnik komunikowania inicjuje odbiór treści, może ustalać zakres i kolejność odbieranych przekazów, a także wpływać na te przekazy i dodawać do nich swoje.

Nowe możliwości i formy komunikacji w Internecie powodują, że praktycznie każdy może być niezależnym wydawcą i publikować w sieci (przykład rozwijających się w rekordowym tempie internetowych blogów[2], podcastingu, czyli własnych audycji internautów rejestrowanych w przyjaznym dla internetowej dystrybucji formacie mp 3 czy vblogingu - tworzenia autorskich serwisów wzbogaconych o sekwencje dźwiękowe i wideo, które inni użytkownicy mogą „prenumerować" na swoje komputery).

Taka rozmaitość form i odmian zawartości, a zwłaszcza krzyżujących się i komplementarnych wobec siebie typów komunikacji i form jej rozpowszechniania rodzi liczne trudności prawne i regulacyjne. Kształt i zakres prawa, któremu powinna podlegać zawartość Internetu stanowi obecnie przedmiot ożywionej międzynarodowej debaty. Toczy się ona na poziomie praw krajowych i wszystkich zainteresowanych stron, w tym międzynarodowych organizacji pozarządowych, dostawców dostępu, treści i usług jak i samych użytkowników Internetu.

Jednocześnie debata ta toczy się na poziomie prawa wspólnotowego. Jednym z pól tej debaty są prace nad nowelizacją unijnej dyrektywy o telewizji bez granic. Traci już aktualność stosowany dotąd przez Unię Europejską, podział na :

- *broadcasting*, czyli nadawanie radiowe i telewizyjne, które na poziomie wspólnotowym reguluje dyrektywa o telewizji bez granic;
- usługi Społeczeństwa Informacyjnego (usługi teleinformatyczne) podlegające dyrektywie o handlu elektronicznym.

W pracach nad nową dyrektywą przewiduje się, że będzie ona regulowała już nie telewizję, ale linearne i nielinearne „usługi audiowizualne" (*audiovisual content services*),

[2] „Co sekundę powstaje nowy blog" – informuje Gazeta Wyborcza z 3.08.2005 r. odnotowując prawie podwojenie liczby internetowych dzienników w pierwszej połowie 2005 r.

niezależnie od środków technicznych ich upowszechniania. Usługi „linearne" to tradycyjne programy telewizyjne. Usługi „nielinearne" to usługi dostarczające zawartość audiowizualną na zamówienie.

Koncepcja ta stała się przyczyną ożywionej dyskusji między państwami członkowskimi, m.in. w kwestii definicji owych „nielinearnych usług audiowizualnych", oraz protestów państw, które postrzegają zagrożenie objęcia zakresem nowej dyrektywy wszelkiej audiowizualnej zawartości Internetu. O ile – w imię zasady neutralności technologicznej – nie kwestionuje się w tej dyskusji objęcie regulacją tradycyjnych programów telewizyjnych dostępnych w Internecie, o tyle niepokój budzi rozszerzenie zakresu dyrektywy na pozamedialne usługi audiowizualne w Internecie.

Zabierając głos w tej dyskusji, Krajowa Rada Radiofonii i Telewizji wskazała, że propozycje Komisji Europejskiej „nie podają *ratio legis* objęcia regulacją wszelkich nielinearnych usług audiowizualnych o pozamedialnym charakterze" i stwierdziła:

> „O ile podejście neutralne technologicznie uzasadnia objęcie wszelkich form telewizji dostępnych w Internecie takim samym zakresem regulacji, jak w przypadku innych platform rozpowszechniania (naziemnej, kablowej czy satelitarnej), o tyle obejmowanie regulacją internetowych usług audiowizualnych o charakterze pozamedialnym wymaga szczególnego uzasadnienia. „Issues Paper" nie wyklucza takiej możliwości, a tym samym sprawia wrażenie, że nowa dyrektywa obejmie wszelkie formy działalności audiowizualnej w Internecie. Ta niejasność musi być usunięta poprzez wykluczenie tej opcji – co jednak nie usuwa możliwości promowania samo- i współregulacji dostawców usług i zawartości internetowej" [3].

Zgodnie z propozycją KRRiT, Komisja Europejska zmieniła podejście do zakresu przedmiotowego nowej dyrektywy [4]. Obecnie dotyczy ona „audiovisual media services", co powinno usunąć niebezpieczeństwo rozszerzenia zakresu na zawartość audiowizualną Internetu nie stanowiącą „usługi medialnej".

---

[3] „Przedmiotowy i terytorialny zakres dyrektywy", Stanowisko Krajowej Rady w sprawie dokumentów problemowych przedstawionych przez Komisję Europejską w ramach procesu konsultacji dotyczących zmiany dyrektywy „Telewizja bez granic", przyjęte przez KRRiT na posiedzeniu w dn. 1 września 2005 r., www.krrit.gov.pl.

[4] Por. projekt nowej dyrektywy oraz liczne materiały towarzyszące na stronie internetowej Dyrekcji Generalnej KE ds. Społęczeństwa Informacyjnego i Mediów:
http://europa.eu.int/information_society/newsroom/cf/itemlongdetail.cfm?item_id=2343

Jest to tylko jeden przykład problemów wynikających na tle debaty o zawartości Internetu.

c) Internet jako przedmiot polityki międzynarodowej - zarządzanie Internetem (*Internet Governance*)

Warto zauważyć, że jak na „sferę nieograniczonej wolności", Internet jest przedmiotem niezwykle zaciętej batalii związanej z jego administrowaniem i zarządzaniem oraz z określaniem zasad, które powinny w nim obowiązywać. Toczy się ona między innymi w organizacjach i instytucjach międzynarodowych, co nieuchronnie nadaje tej batalii charakteru politycznego. Tabela nr 1 ilustruje liczbę oraz charakter tych instytucji i organizacji, które zajmują się zarządzaniem w zakresie poszczególnych obszarów technologii informacyjno-komunikacyjnych *(ICT*).

Tabela nr 1. Udział różnych organizacji i instytucji w formułowaniu polityki międzynarodowej w zakresie technologii informacyjno-komunikacyjnych (ICT)

Dziedzina	Sfery polityki	Organizacje
Konwergencja i cyfryzacja	Przydział widma częstotliwości bezprzewodowych i radiowych (nowe usługi, harmonizacja pasm częstotliwości, itp.)	ITU *
	Dostęp warunkowy i interoperacyjność (wąskie gardło, ułatwienia o zasadniczym znaczeniu, anty-koncentracja, wyłaniające się standardy, itp.)	ITU / IETF, W3C / WTO / GBDe
	Powszechne Identyfikatory (nazwy domenowe, ENUM - rejestracja w systemie nazw domenowych numerów telefonów, identyfikatory obiektowe, itp.)	ICANN / IETF / WIPO
	Reforma regulacyjna (zredefiniowanie obszarów regulacyjnych, konwergentni regulatorzy, itp.)	Różne, w tym Bank Świato-wy i MFW
Gospodarka sieciowa	Ochrona konsumenta (rozwiązywanie konfliktów ponadgranicznych, kwestie jurysdykcyjne, itp.)	OECD / ITU /WIPO / UNCITRAL/ GBDe
	Umowy elektroniczne i podpis elektroniczny (autentyfikacja, standardy, prawa modelowe, itp.)	UNCITRAL / IETF / W3C / OECD
	Własność intelektualna (*copyright*, znaki towarowe, odpowiedzialność dostawców usług internetowych – *ISP,* itp.)	WIPO / ICANN / WTO
Społe-czeństwo Informacyjne	Bezpieczeństwo sieci (cyberprzestępczość, hakerstwo, infrastruktura krytyczna, itp.)	ICANN /ITU / OECD / CoE
	Różnorodność kulturowa i językowa (wielojęzyczność nazw domenowych, różnorodność zawartości, itp.)	ICANN / ITU / WIPO/ UNESCO / CoE
	Warunki rynkowe (technologie informacyjno-telekomunikacyjne w handlu, polityka cenowa, dostępne dane wejściowe, kredyty, podatki, itp.)	WTO / UNCTAD

Opracowano na podstawie: Implementation Team on Global Policy Participation, A Roadmap: Global Policymaking for Information and Communications Technologies Enabling Meaningful Participation by Developing-Nation Stakeholders New York: G8 Digital Opportunity Task Force, 2002.
** Objaśnienie skrótów użytych w tabeli nr 1 – patrz Załącznik nr 1.*

Jeśli chodzi o techniczne funkcje zarządzania Internetem (rejestracja, zarządzanie i koordynacja systemem nazw domen, czyli tzw. systemem DNS) z racji historycznych uwarunkowań, kompetencje w tym zakresie należą do USA. Na mocy umowy z amerykańskim rządem funkcję tę sprawuje Internetowa Korporacja ds. Przydzielonych Nazw i Numerów (*The Internet Corporation for Assigned Names and Numbers* - ICANN) [5]. Instytucja ta odpowiedzialna jest za przyznawanie nazw domen internetowych, ustalanie ich struktury oraz za ogólny nadzór nad działaniem serwerów DNS na całym świecie.

Formalnie jest to prywatna organizacją non-profit, o statusie firmy zarejestrowanej w stanie Kalifornia, której rząd USA przekazał czasowo prawo nadzoru nad systemem DNS i przydziałem puli adresów IPv4 oraz IPv6 dla tzw. *Regional Internet Registers* (RIR) oraz rejestrację numerów portów. Autonomiczną częścią ICANN jest IANA (*Internet Assigned Number Authority)*, która obecnie zarządza tylko „szczytowymi" domenami i sprawuje ogólny nadzór nad działaniem mechanizmu DNS. Rada ICANN wypracowuje jednomyślne podejście do polityki i spraw związanych z systemem DNS prowadząc konsultacje w ramach swoich trzech organizacji wspierających, które reprezentują szeroki wachlarz grup interesów - przedsiębiorstwa, konsumentów i dostawców usług internetowych (*ISP*).

Z powodu pełnienia kluczowych technicznych funkcji koordynacyjnych, ICANN wywiera silny wpływ na politykę publiczną. Korzysta przy tym z wkładu rządowego ze strony Rządowego Komitetu Doradczego (GAC). GAC doradza przede wszystkim w tych sprawach, w których polityka prowadzona przez ICANN oraz prawa narodowe lub umowy międzynarodowe mogą wzajemnie na siebie wpływać. Obecnie w Komitecie GAC regularnie uczestniczy ponad 30 rządów narodowych, odrębnych systemów gospodarczych oraz wielonarodowych organizacji rządowych i organizacji traktatowych (między innymi Międzynarodowy Związek Telekomunikacyjny ITU, czy WIPO). Członkowie tego Komitetu mogą zatem wpływać na politykę odnośnie zarządzania systemem DNS, a przez to na odpowiednie funkcje istotne dla ogólnego funkcjonowania Internetu [6].

Opisany powyżej system nie znajduje jednak akceptacji ze strony wszystkich krajów: coraz silniej brzmią publicznie wyrażane głosy domagające się wypracowania nowego

[5] Więcej informacji o ICANN : www.icann.org

[6] Więcej informacji o Rządowym Komitecie Doradczym korporacji ICANN: www.gac.icann.org

porozumienia w sprawie podziału ról i zakresów odpowiedzialności wszystkich stron w systemie zarządzania Internetem, a nie tylko USA, czy szerzej - państw wysoko rozwiniętych. Chodzi przede wszystkim o wypracowanie równoprawnego udziału państw rozwijających się. Jest to obecnie przedmiot zaciekłej międzynarodowej debaty, a stawką jest zapewnienie przyszłości i bezpieczeństwa Internetu w świetle podziału wpływów między sferę biznesu a sfery polityki publicznej. Głównym dylematem jest pytanie o skalę i zakres udziału rządów państw (państw o jakich ustrojach politycznych i gospodarczych? wszystkich państw bez wyjątku? Jeśli tak, to jaki podział głosów zastosować?) w zarządzaniu Internetem.

Efektem tej debaty było powołanie przez Sekretarza Generalnego ONZ na podstawie mandatu otrzymanego podczas pierwszej fazy Światowego Szczytu ds. Społeczeństwa Informacyjnego (Genewa, grudzień 2003 r.) tzw. Grupy Roboczej ds. Zarządzania Internetem (*Working Group on Internet Governance*), złożonej z 40 przedstawicieli rządów, sektora prywatnego i przedstawicieli społecznych. Owocem prac tej Grupy jest raport z czerwca 2005 r., którego propozycje stanowiły przedmiot obrad drugiej fazy Światowego Szczytu ds. Społeczeństwa Informacyjnego (Tunis, 16-18.11. 2005 r.) [7].

Raport ten zawiera następującą definicję zarządzania Internetem: „Zarządzanie Internetem to przyjęcie i stosowanie, odpowiednio i zgodnie z pełnioną przez siebie rolą, przez rządy, sektor prywatny i społeczeństwo obywatelskie wspólnych zasad, norm, przepisów, procedur decyzyjnych i programów działania, które kształtują ewolucję i wykorzystanie Internetu".

Raport przedstawił także listę czterech głównych dziedzin polityki publicznej w skali krajowej i międzynarodowej w zakresie Internetu:

- Sprawy związane z infrastrukturą i zarządzaniem kluczowymi zasobami Internetu, w tym administracją domen i adresów IP, administrowaniem systemem serwerów głównych (*root server systems*), wymianą ruchu pomiędzy dostawcami usług internetowych na zasadzie partnerstwa (*peering)* oraz interkonektem, a także infrastrukturą telekomunikacyjną, w tym technologiami konwergentnymi oraz zapewnieniem wielojęzyczności Internetu;
- Sprawy związane z wykorzystaniem Internetu, w tym spamu, bezpieczeństwa sieci i cyberprzestępczości;
- Własność intelektualna i handel międzynarodowy;

[7] Report of the Working Group on Internet Governance, Château de Bossey June 2005, http://www.wgig.org/docs/WGIGREPORT.pdf

- Internet a rozwój, w tym rozbudowa zdolności korzystania z Internetu w krajach rozwijających się.

Inne sfery polityki publicznej określone przez Grupę Roboczą to:

- Zdolność do uczestnictwa w tworzeniu polityki globalnej w zakresie Internetu;
- Swoboda wypowiedzi;
- Ochrona danych i prywatności;
- Prawa konsumentów;
- Konwergencja;
- Sieci następnej generacji;
- E-handel.

Raport ten rekomenduje między innymi stworzenie „nowej przestrzeni do równoprawnego dialogu wszystkich stron w zakresie wszelkich kwestii odnoszących się do zarządzania Internetem. Jeśli chodzi o rolę i zakres odpowiedzialności państw, Grupa Robocza uważa, że żaden rząd nie powinien samoistnie pełnić dominującej roli w zarządzaniu Internetem na forum międzynarodowym oraz postuluje wzmocnienie roli państw rozwijających się w tym zakresie. Jednocześnie Grupa zaproponowała cztery możliwe rozwiązania w zakresie zarządzania Internetem:

- stworzenie umocowanej przy ONZ Światowej Rady Internetu składającej się z członków rządów narodowych w liczbie adekwatnej do podziału regionalnego oraz z innych właściwych przedstawicieli. Rada ta przejęłaby od amerykańskiego Departamentu Handlu funkcje międzynarodowego zarządzania Internetem oraz zastąpiłaby działający przy ICANN Rządowy Komitet Konsultacyjny (GAC);
- wzmocnienia roli wyżej wymienionego Rządowego Komitetu Konsultacyjnego (GAC) w oparciu o równoprawne uczestnictwo wszystkich stron w ramach światowego Forum wymiany i dialogu, co zapewni efektywny i użyteczny wkład państw rozwijających się w mechanizm zarządzania Internetem;
- utworzenie Międzynarodowej Rady Internetu, która, między innymi, przejęłaby kompetencje ICANN oraz GAC;
- rozdzielenie 3 kluczowych kompetencji w zakresie zarządzania Internetem między trzy różne, nowe instancje, w tym Radę ds. Światowej Polityki w zakresie Internetu

(CPIM) oraz WICANN (*Word Internet Corporation...*) powstały na bazie zreformowanego i umiędzynarodowionego ICANN.

W debacie na ten temat [8], Unia Europejska przedstawiła koncepcję, zgodnie z którą niezależny ICANN byłby nadzorowany jedynie przez regularne spotkania ciała międzyrządowego, zajmującego się wyłącznie kwestiami technicznymi, a dodatkowo powołano by otwarte dla wszystkich forum związane z ONZ, poświęcone omawianiu problematyki związanej z zarządzaniem Internetem [9]. Tym samym, Unia Europejska, której stanowisko w sprawie zarządzania Internetem zostało określone na spotkaniu Rady Ministrów UE w dniach 27-28 czerwca 2005 r. opowiedziała się za nowym, publiczno-prywatnym modelem współpracy (*the new public-private co-operation model)* w zakresie zarządzania Internetem*,* który opierałby się na bardziej demokratycznych, przejrzystych i wielostronnych zasadach niż dotychczasowy mechanizm oraz kładł większy nacisk na korzyści wynoszone przez politykę publiczną wszystkich rządów, ale który jednocześnie:

- nie zastępowałby istniejących już mechanizmów ani instytucji, lecz zbudowany byłby na fundamencie tych ostatnich, z położeniem silniejszego nacisku na komplementarność pomiędzy wszystkimi stronami tego procesu, włączając w to rządy państw, sektor prywatny, społeczeństwo oraz organizacje międzynarodowe";
- przyczyniałby się do utrzymującej się stabilności i silnego rozwoju Internetu poprzez powiązanie polityki publicznej z kluczowymi elementami zarządzania Internetem [10].

W ostatecznym efekcie, kompromis [11] zawarty w ostatniej chwili tuż przed rozpoczęciem drugiej fazy Światowego Szczytu Społeczeństwa Informacyjnego (Tunis, 16-

[8] Wiele głosów oponowało przeciwko ustanowieniu mechanizmu regulacji Internetu kontrolowanego przez rządy państw. Carl Bildt, były premier Szwecji (Carl Bildt, "Keep the Internet free", International Herald Tribune, 11.10.2005 r.) stwierdził, że oznaczałoby to nie tylko korzystne dla autorytarnych reżimów ograniczanie wolności, jaką wnosi Internet, ale także dławienie innowacji i zagrożenie bezpieczeństwa całego systemu. Według Bildta, sama próba stworzenia takiego mechanizmu mogłaby spowodować konflikty i doprowadzić do bałkanizacji globalnej sieci, czyli powstania różnych, mniej lub bardziej zamkniętych, systemów. Jego zdaniem, „Europejczycy powinni szczególnie dbać o system, który działa zadziwiająco dobrze, nawet jeśli oznacza to pozostawienie niektórych funkcji kontrolnych w rękach USA, co według niego jest z pewnością lepszym rozwiązaniem niż oddanie sterów teokratom i autokratom z całego świata".

[9] Por. "Towards a Global Partnership in the Information Society: The Contribution of the European Union to the Second Phase of the World Summit on the Information Society (WSIS)". COM(2005) 234 final Brussels, 02.6.2005. http://europa.eu.int/information_society/activities/internationalrel/docs/wsis/com02062005_en.pdf.

[10] Initial Comments by the European Union and the acceding countries Romania and Bulgaria, on the report of the Working Group on Internet Governance, Document WSIS-II/PC-3/CONTR/19-E, 1 August 2005.

[11] President of the PrepCom of the Tunis Phase, "Tunis Agenda For The Information Society". Document: WSIS-05/TUNIS/DOC/6(Rev.1)-E 15 November 2005, http://www.itu.int/wsis/docs2/tunis/off/6rev1.doc

18.11.2005 r.) - i potwierdzony podczas samego szczytu - przewiduje pozostawienie ICANN w obecnej formie, natomiast powołanie Forum Zarządzania Internetem (*Internet Governance Forum*), z udziałem przedstawicieli rządów, sektora prywatnego i społeczeństwa obywatelskiego, którego zadaniem będzie prowadzenie dialogu na temat polityki publicznej i międzynarodowej w odniesieniu do Internetu oraz takich problemów jak spam, wirusy komputerowe i cyberprzestepczość. Jego pierwsze posiedzenie zostanie zwołane przez Sekretarza Generalnego ONZ w pierwszej połowie 2006 r. w Atenach.

Zawarte porozumienie przewiduje też bardziej aktywną współpracę międzyrządową na temat polityki w odniesieniu do Internetu w celu wypracowania wspólnych zasad tej polityki. Dokonuje ono też swoistego „przydziału" poszczególnych sfer polityki w dziedzinie Internetu społeczności międzynarodowej i poszczególnym organizacjom międzynarodowym. Ilustruje to Tabela nr 2.

Tabela nr 2. Pola specjalizacji i działalności poszczególnych organizacji międzynarodowych w zakresie polityki w dziedzinie Internetu

Sfera polityki	Organizacje międzynarodowe
Rola władzy publicznej i innych podmiotów w promocji wykorzystania ICT na rzecz rozwoju	ECOSOC / Regionalne Komisje ONZ / ITU *
Infrastruktura informacyjna i komunikacyjna	ITU
Dostęp do informacji i wiedzy	ITU / UNESCO
Rozwój zdolności korzystania z Internetu	UNDP / UNESCO / ITU / UNCTAD
Wspierania zaufania i bezpieczeństwa korzystania z ICT	ITU
Tworzenie korzystnych warunków dla rozwoju i wykorzystania Internetu	ITU / UNDP / Regionalne Komisje ONZ / UNCTAD
Zastosowania ICT • E-government • E-business • E-learning • E-health • E-employment • E-environment • E-agriculture • E-science	 UNDP / ITU WTO / UNCTAD / ITU / UPU UNESCO / ITU / UNIDO WHO / ITU ILO / ITU WHO / WMO / UNEP / UN- Habitat /ITU/ICAO FAO / ITU UNESCO / ITU / UNCTAD
Różnorodność kulturowa i tożsamość, różnorodność językowa, lokalna zawartość	UNESCO
Media	UNESCO
Etyczny wymiar społeczeństwa informacyjnego	UNESCO / ECOSOC
Współpraca międzynarodowa i regionalna	Regionalne Komisje ONZ/ UNDP /ITU/ UNESCO / ECOSOC

** Objaśnienie skrótów użytych w Tabeli nr 2 – patrz Załącznik nr 1.*

Źródło: Dokument WSIS-05/TUNIS/DOC/6 (Rev.1)-E, 15 November 2005, Tunis Agenda for the Information Society, http://www.itu.int/wsis/docs2/tunis/off/6rev1.html

2. SWOBODA WYPOWIEDZI I INFORMACJI W INTERNECIE: RÓŻNICE PODEJŚĆ

Z punktu widzenia niniejszego opracowania, można wyróżnić trzy główne podejścia do kwestii zawartości Internetu i jej regulacji:

- odmowa uznania jakichkolwiek ograniczeń swobody wypowiedzi i informacji w Internecie;
- kontrola i cenzura w Internecie;
- dążenie do osiągnięcia równowagi między swobodą komunikowania w Internecie a innymi prawami i swobodami człowieka przyjmując jako punkt odniesienia ochronę małoletnich i godności ludzkiej.

Poniżej omówimy praktyczne przykłady tych postaw i konsekwencji wcielania ich w życie.

a) Państwo nie powinno wprowadzać ograniczeń i regulacji zawartości Internetu

Postawę tego typu reprezentują takie organizacje jak Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE) czy branżowa międzynarodowa organizacja z zakresu monitoringu wolności słowa i mediów „Reporterzy bez Granic".

OBWE nie ma kompetencji do stanowienia prawa ani działania bez uprzedniej zgody państw członkowskich, niemniej jednak jej głos jako powszechnie znanej i szanowanej organizacji międzynarodowej zrzeszającej 55 państw jest uwzględniany na forum międzynarodowym. Jej stanowisko w sprawie ograniczania swobody wypowiedzi w Internecie polega na wyraźnym sprzeciwie wobec ingerencji państw w zawartość tego medium. Rekomendacje Amsterdamskie OBWE „Wolność prasy a Internet" z 2003 r. stwierdzają między innymi, że do Internetu należy odnosić te same wszystkie zasady swobody wypowiedzi, co do mediów tradycyjnych. Stosowanie wszelkich mechanizmów filtrowania czy blokowania zawartości, bądź innych form cenzury, jest niedopuszczalne. Wprawdzie nie można tolerować wykorzystywania Internetu do celów przestępczych, jednak działania prawne czy policyjne powinny być zorientowane na nielegalną zawartość, nie zaś na Internet jako taki. Internet, stwierdza dalej dokument OBWE, może być wykorzystywany do różnych celów i wszelkie działania państw muszą jasno odróżniać komunikację porozumiewawczą (prywatną) od publicznej.

Stanowisko OBWE wobec Internetu podzielają i wspierają Reporterzy bez Granic**.** W czerwcu 2005 r. obie organizacje wspólnie wydały Deklarację zawierającą 6 zaleceń w celu zagwarantowania swobody wypowiedzi w Internecie. Deklaracja ta powstała jako przyczynek do dyskusji na Światowy Szczyt Społeczeństwa Informacyjnego (Tunis, 16-18 listopada 2005 r.). W intencji autorów Deklaracji, odnosi się ona do wszystkich krajów, a nie tylko krajów europejskich.

Poniżej pełny tekst Deklaracji:

1) Każde prawo dotyczące przepływu informacji w Internecie musi opierać się zasadach swobody wypowiedzi, zdefiniowanej w art. 19 Powszechnej Deklaracji Praw Człowieka;
2) W otwartym i demokratycznym społeczeństwie każdy obywatel może decydować o informacjach, do których chce mieć dostęp za pomocą Internetu. Niedopuszczalne jest filtrowanie lub *rating* (ocenianie) zawartości *online* przez rząd. Filtry mogą by instalowane wyłącznie przez samych internautów. Każda procedura filtrująca na wyższym (lokalnym lub krajowym) poziomie jest sprzeczna z zasadą swobody przepływu informacji.
3) Niedopuszczalny jest obowiązek rejestracji stron internetowych przez jednostki administracji publicznej. W przeciwieństwie do koncesji radiowo-telewizyjnych, uzasadnionych ograniczoną ilością częstotliwości, koncesjonowanie Internetu nie znajduje uzasadnienia, a to z powodu nieograniczonych zasobów, na których opiera się jego infrastruktura. Przeciwnie, obowiązkowa rejestracja publikacji *online* stwarza ryzyko stłumienia wolnej wymiany myśli, opinii i informacji w Internecie;
4) Techniczny dostawca Internetu nie może być uznawany za odpowiedzialnego za zwykłą transmisję (*conduit*) lub hosting zawartości, chyba, że odmawia on podporządkowania się decyzji sądu. Decyzja dotycząca legalności lub nielegalności danej strony internetowej może być bowiem podjęta wyłącznie przez sąd, w żadnym przypadku przez technicznego dostawcę Internetu. Taka procedura prawna powinna zagwarantować zasady przejrzystości i odpowiedzialności oraz prawo do odwołania;
5) Każda treść przekazywana przez Internet powinna podlegać wyłącznie jurysdykcji kraju pochodzenia *(upload rule)* a nie kraju, w którym jest pobierana;
6) Internet łączy różnego typu formy medialne oraz rozwija nowe narzędzia publikacji, takie jak blogi. Osoby piszące w Internecie oraz internetowi dziennikarze muszą

korzystać z podstawowego prawa do swobody wypowiedzi oraz dodatkowo z prawa do prywatności i poufności źródeł.

Także Kanada nie uznaje jakiejkolwiek konieczności regulacji prawnej tego medium, co przejawia się również decyzją o nie rozciąganiu regulacji nawet na te usługi internetowe, które można by objąć definicją radiofonii i telewizji. Używa przy tym argumentu, że objęcie ich regulacją i koncesjonowaniem nie przyczyniłoby się do ich rozwoju oraz nie zwiększyłoby korzyści, jakie Kanadyjczycy odnoszą z korzystania z Internetu. W 1999 r. Komisja ds. Radia, Telewizji i Telekomunikacji podjęła decyzję w tej sprawie [12], uznając, że webcasting nie jest jeszcze substytutem telewizji.

b) Stanowisko pośrednie (Unia Europejska i Rada Europy)

Jednoznacznego i bezkompromisowego stanowiska OBWE i Reporterów bez Granic w zakresie braku powodów do ograniczania swobody wypowiedzi i informacji w Internecie nie podzielają inne międzynarodowe organizacje, takie jak Unia Europejska czy Rada Europy. Ukazuje to jedną, zasadniczą linię podziału debaty na zwolenników i przeciwników stosowania ograniczeń. Druga linia podziału – już w łonie samych zwolenników powyższych ograniczeń - dotyczy zakresu tychże oraz przesłanek im przyświecających, a także stosowanych w tym celu metod, które siłą rzeczy zahaczają o relacje prawo - Internet.

Jeśli chodzi o Unię Europejską i Radę Europy, opowiadają się one za kontrolowaną i ograniczoną ingerencją swoich państw członkowskich w swobodę wypowiedzi i informacji w Internecie, a podejście to realizują za pomocą instrumentów prawnych lub politycznych, czemu przyświecają następujące przesłanki:

- Dopuszczalne ograniczenia w zakresie swobody wypowiedzi i informacji w Internecie ze względu na szczególne okoliczności zewnętrzne (bezpieczeństwo publiczne);
- Dopuszczalne ograniczenia w zakresie swobody wypowiedzi i informacji w Internecie ze względu na potrzebę ich zrównoważenia z innymi prawami i swobodami obywatelskimi.

[12] Por. „New Media", Broadcasting Public Notice CRTC 1999-84, Telecom Public Notice CRTC 99-14, 17 May 1999, http://www.crtc.gc.ca/eng/bcasting/notice/ 1999/P9984_0.txt

c) Kraje autokratyczne: zaprzeczenie zasady swobody wypowiedzi i informacji w Internecie

Skrajnym przykładem całkowicie odmiennego podejścia, zaprzeczającego zasadzie swobody wypowiedzi i przepływu informacji w Internecie, jest model stosowany w krajach niedemokratycznych. Organizacja Reporterzy bez Granic do „wrogów Internetu" zalicza obecnie 15 następujących państw: Tunezję (gospodarza drugiej fazy Szczytu Społeczeństwa Informacyjnego): Białoruś, Birmę, Chiny, Kubę, Iran, Libię, Malediwy, Nepal, Koreę Północną, Arabię Saudyjską, Syrię, Turkmenistan, Uzbekistan i Wietnam.

Władze wielu z tych krajów stosują ścisłą regulację Internetu korzystając z takich metod jak: pełna kontrola treści przekazywanych przez krajowych dostawców treści, wzmocniona wymogiem korzystania z państwowych dostawców usług mających zdolność cenzurowania treści, technologie filtrujące i blokujące dostęp do treści uważanych za wywrotowe politycznie, w tym blokowanie zagranicznych stron internetowych, filtrowanie zawartości, w tym kluczowych słów, witryn internetowych i forów dyskusyjnych, rejestracja wszystkich działających stron internetowych i blogów umożliwiająca pełną identyfikację i kontrolę osób za nie odpowiedzialnych, monitorowanie poczty elektronicznej i internetowych kawiarenek, osobistych komputerów, rozsyłanie wirusów i łączenie z systemami monitorowania bezpieczeństwa publicznego, obowiązek korzystania z państwowych wyszukiwarek, system oficjalnych zezwoleń na dostęp do Internetu pod karą grzywny lub więzienia.

Model ten stanowi przykład całkowitego podporządkowania komunikacji w Internecie wewnętrznemu systemowi cenzury stosowanemu przez dany kraj w celach politycznych. Na współpracę z rządami tych państw idą nawet wielcy światowi producenci oprogramowania i wielkie portale internetowe [13]. Ich postawę piętnują obrońcy praw człowieka i wolności mediów jako przykład przedkładania względów ekonomicznych nad fundamentalne prawa człowieka.

[13] Por: Chińska internetowa dyktatura, Rzeczpospolita, 05.06.2005 r. oraz Zbigniew Domaszewicz, Autocenzura Microsoftu w Chinach, Gazeta Wyborcza, 15.06. 2005 r., a także Microsoft pomaga cenzurować chiński Internet, Wirtualne Media, 16.06.2005 r. Por. także http://wirtualnemedia.pl/document.php?id=332376 oraz http://www.rsf.org/article.php3?id_article=10757 i http://www.journaldunet.com/cgi/printer/index.cgi.

3. SWOBODA WYPOWIEDZI I INFORMACJI W INTERNECIE A WALKA Z TERRORYZMEM

a) Unia Europejska

Zagrożenie ze strony międzynarodowego terroryzmu oraz dążenie wielu krajów do wzmocnienia walki z tym zjawiskiem traktowane jest przez wiele rządów jako uzasadnienie dla ograniczania praw człowieka i swobód obywatelskich. W trakcie dyskusji w łonie Unii Europejskiej na temat tzw. „data retention" (obowiązek przedsiębiorstw telekomunikacyjnych i internetowych do przechowywania danych o wszelkich połączeniach nawiązywanych przez ich klientów) brytyjski minister spraw wewnętrznych próbował przekonać zarówno eurodeputowanych w Strasburgu jak i zgromadzonych w Londynie ministrów, że projekt jest „fundamentalny dla bezpieczeństwa Europy i że państwa Unii muszą zaakceptować erozję niektórych praw obywatelskich, jeśli ich obywatele mają być chronieni przed przestępczością zorganizowaną i terroryzmem". Dodał również, że „równowaga między prawami jednostki i potrzebami bezpieczeństwa jest nieprawidłowa". Można by to traktować wręcz jako wezwanie do zmiany Europejskiej Konwencji Praw Człowieka [14].

b) USA

Tezę o zaistnieniu szczególnych okoliczności uzasadniających ograniczenie swobody wypowiedzi i przepływu informacji w Internecie ilustruje przykład Stanów Zjednoczonych**.** Jest to kraj powszechnie utożsamiany z wolnością słowa (wypowiedzi) i gwarantującą to Pierwszą Poprawką do Konstytucji. Amerykańska *Federal Communications Commission* głosiła zasadę [15], że najlepszym podejściem do Internetu jest leseferyzm, czyli brak wszelkiej regulacji i że właśnie taka postawa władz amerykańskich pozwoliła na jego ogromny i bardzo szybki rozwój w Stanach Zjednoczonych.

Jednak okoliczności, o których mowa wynikają z wydarzeń 11 września 2001 r. i następujących po nich dążeń USA do wzmocnienia walki z terroryzmem. Skłoniły one USA do wprowadzenia kompleksowego systemu nadzoru nad zawartością w Internecie, systemu,

[14] Źródło: UE: Telefoniczne prawo antyterrorystyczne? Wirtualne Media, 09.09.2005 r. ; Por: UE: Spór o kontrolowanie internautów, Onet Wiadomości, 13.06.2005r. oraz UE będzie rejestrować e-maile i smsy?, Wirtualne Media, 14.07.2005 r.

[15] J. Oxman, „The FCC and the Unregulation of the Internet", http://www.fcc.gov

który działa na podstawie ustawy „*Patriot Act*” [16] (liczne jego przepisy odnoszą się do komunikacji elektronicznej i nadzoru nad nią) i wzbudza protesty zarówno międzynarodowej organizacji Reporterzy bez Granic jak i licznych amerykańskich organizacji broniących swobód obywatelskich.

Tendencja ta spotyka się z reakcją wskazującą na konieczność ochrony praw człowieka w każdych okolicznościach.

c) Rada Europy

Z kolei, przyjęte przez Radę Europy w 2002 r. „Wytyczne w zakresie praw człowieka i walki z terroryzmem” [17] poruszają kwestię poszanowania życia prywatnego osób w związku z gromadzeniem i przetwarzaniem danych osobistych (wytyczna nr V) przez kompetentne władze w zakresie bezpieczeństwa kraju. Aby poszanowanie to miało miejsce, muszą być spełnione 3 następujące warunki:

- umocowanie w prawie krajowym;
- proporcjonalność wobec celu, któremu ten zabieg służy;
- poddanie kontroli przez niezależny organ zewnętrzny.

W 2005 r. Komitet Ministrów Rady Europy przyjął “Deklarację nt. swobody wypowiedzi i informacji w kontekście walki z terroryzmem” [18], w której między innymi wzywa państwa członkowskie:

- nie wprowadzały nowych ograniczeń swobody w mediach, chyba, że jest to niezbędne i proporcjonalne w społeczeństwie demokratycznym;
- nie utożsamiały informacji o terroryzmie ze wspieraniem terroryzmu;
- zapewniały dostęp dziennikarzy do informacji;
- powstrzymywały się od niepotrzebnego blokowania dostępu dziennikarzy do miejsc, w których zaszły akty terrorystyczne;

[16] Źródło: http://www.journaldunet.com/cgi/printer/index.cgi
[17] „Guidelines on Human Rights and the Fight Against Terrorism”, Strasbourg: Council of Europe, 2002, http://www.coe.int/T/E/Human_rights/h-inf(2002)8eng.pdf
[18] “Declaration on freedom of expression and information in the media in the context of the fight against terrorism” https://wcd.coe.int/ViewDoc.jsp?Ref=Dec-02.03.2005&Sector=secCM&Language= lanEnglish&BackColorInternet= 9999CC&BackColorIntranet=FFBB55&BackColorLogged=FFAC75

- zagwarantowały prawo dziennikarzy do uzyskania informacji o zarzutach postawionych osobom oskarżonym o działania terrorystyczne oraz do informowania o śledztwie i przewodzie sądowym;
- szanowały prawo dziennikarzy do nie ujawniania źródeł informacji;
- szanowały niezależność redakcyjną mediów i nie wywierały na nie żadnej presji.

d) **ARTICLE 19**

Do sprawy ograniczania swobody wypowiedzi w związku z walką z terroryzmem odnosi się także dokument przyjęty w październiku 1995 r. pod egidą międzynarodowej pozarządowej organizacja o nazwie ARTICLE 19 (nazwa wywodzi się z art. XIX Powszechnej Deklaracji Praw Człowieka) - *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information.* Zasady te zostały wypracowane przez grupę ekspertów z zakresu prawa międzynarodowego, bezpieczeństwa narodowego oraz praw człowieka we współpracy z Uniwersytetem w Johannesburgu. Stanowczo przeciwstawiają się one ograniczaniu swobody wypowiedzi i przepływu informacji ze względu na bezpieczeństwo narodowe, niemniej jednak przewidują trzy, ściśle określone, następujące odstępstwa od reguły. Należą do nich przypadki, w których rząd danego kraju będzie w stanie wykazać, że:

- dany przejaw swobody wypowiedzi zmierza do wzbudzenia przemocy;
- występuje prawdopodobieństwo wzbudzenia przemocy;
- występuje bezpośredni i natychmiastowy związek między danym przejawem swobody wypowiedzi a możliwością wzniecenia przemocy.

Ponadto, „Zasady Johannesburskie" bardzo szczegółowo określają liczne prawa osób oskarżonych o przestępstwa związane z zagrożeniem bezpieczeństwa narodowego, a także stwierdzają, że bezpieczeństwo to nie może stanowić przyczyny zmuszania dziennikarzy do ujawnienia poufnych źródeł pozyskanych informacji.

4. DOPUSZCZALNE OGRANICZENIA SWOBODY WYPOWIEDZI I INFORMACJI W INTERNECIE ZE WZGLĘDU NA POTRZEBĘ ICH ZRÓWNOWAŻENIA Z INNYMI PRAWAMI I SWOBODAM OBYWATELSKIMI

Wychodząc z założenia, że swoboda wypowiedzi i informacji w Internecie nie powinna naruszać interesów społecznych, ani zagrażać godności ludzkiej oraz innym prawom i wolności człowieka, szczególnie jeśli chodzi o małoletnich [19], organizacje międzynarodowe takie jak Rada Europy i Unia Europejska, jak też niektóre kraje dopuszczają stosowanie pewnych ograniczeń w zakresie swobody komunikowania w Internecie. Chodzi o to, by zapobiegać nadużywaniu tej swobody w celu upowszechniania treści sprzecznych z prawem (to, co nielegalne *off-line* jest też nielegalne *online*) oraz treści potencjalnie szkodliwych.

a) Zapobieganie treściom nielegalnym i potencjalnie szkodliwym

O ile nie ma większych problemów ze zdefiniowaniem treści nielegalnych, szczególnie jeśli chodzi o pornografię dziecięcą, pedofilię, treści rasistowskie czy ksenofobiczne (choć i tu istnieją krajowe różnice wynikające z różnych porządków prawnych i różnic kulturowych), o tyle nie istnieje uniwersalna definicja treści potencjalnie szkodliwych[20]. Przykładowo, kwalifikują się do nich takie treści jak te umieszczane w internetowych poradnikach dla anorektyków, niedoszłych samobójców czy amatorów konstruowania bomb. Jednak kwalifikacja ta opiera się bardziej na uznaniowości i intuicji niż na obiektywnych kryteriach [21], w związku z czym treści tego rodzaju stanowią duży problem i wyzwanie z prawnego punktu widzenia. O ile przestępstwa popełniane w sieci podlegają ściganiu na mocy prawa karnego lub cywilnego, a ponadto funkcjonuje już i ciągle rozwija międzynarodowy mechanizm służący do ich wychwytywania za pomocą specjalnych linii interwencyjnych „*Hotlines"* (szerzej na ten temat Załącznik nr 2 i 3), o tyle zwalczanie treści

[19] Nieletni stanowią bardzo liczną i aktywną grupę użytkowników Internetu (szacuje się, że spędzają już więcej czasu w Internecie niż przed telewizorem), a jednocześnie z racji wieku są najbardziej narażeni na zagrożenia ze strony dorosłych nadużywających swobody komunikowania w tym medium.

[20] Jedna z grup eksperckich Rady Europy podjęła się opracowania definicji treści szkodliwych. Patrz Raport Rady Europy, MC-S-IS(2005)007, Group of Specialists on Human Rights in the Information Society (MC-S-IS), Harmful content, prepared by Rachel O'Connell, 31.08.2005 r.

[21] Coraz bardziej widoczna staje się tendencja zmierzająca do delegalizowania treści dotychczas uważanych za potencjalnie szkodliwe. Przykłady: 1) na początku 2006 r. w Australii wejdzie w życie przepis o delegalizacji stron internetowych poświęconych samobójstwom; 2) we wrześniu 2005 r. bawarski minister spraw wewnętrznych wezwał do znalezienia sposobu na blokowanie w Internecie dostępu do instrukcji budowy bomb na wzór filtrów blokujących dostęp do dziecięcej pornografii. Źródło: http://www.wirtualnemedia.pl/document.php?id=338793)

potencjalnie szkodliwych jest z wielu względów bardzo utrudnione. Z tego względu, nacisk kładzie się zatem na zapobieganie tego typu treściom poprzez promowanie działań samoregulujących podejmowanych przez dostawców treści i usług. Podobna filozofia (choć wynika ona z innych przesłanek) przyświeca również walce z treściami nielegalnymi. Wkroczenie w tę sferę organów ścigania i prawa karnego stanowi środek ostateczny, działający *ex-post*, czyli po stwierdzeniu przestępstwa, natomiast w przypadku pedofilii czy pornografii dziecięcej w Internecie, nadrzędnym wyzwaniem jest przeciwdziałanie powstawaniu tych zjawisk. Unia Europejska czy Rada Europy wraz z państwami członkowskimi, jak też niektóre inne kraje kładą nacisk nie tyle na zwalczanie, ile na zapobieganie treściom nielegalnym i potencjalnie szkodliwym. Czynią to poprzez promowanie bezpiecznego korzystania z Internetu, wykorzystując do tego celu różne, opisane w niniejszym opracowaniu, środki i mechanizmy. Jednocześnie obserwuje się też coraz większą społeczną i polityczną percepcję wyżej wymienionych zagrożeń, co przekłada się na coraz większą aktywność poszczególnych państw i organizacji w tym zakresie. Nawet kraje przodujące dotychczas w realizacji podejścia polegającego na braku jakiejkolwiek regulacji Internetu jako przejawu polityki państwa, wykazują pierwsze oznaki zmiany kursu. Różnice między nimi i linia podziału prowadzonej przez nie debaty dotyczy między innymi relacji między prawem a Internetem, które to relacje mogą kształtować się na 3 następujących poziomach:

- ogólnym (prawo ogólne znajduje zastosowanie również do Internetu);
- szczegółowym (tworzy się regulacje prawne mające zastosowanie wyłącznie do Internetu lub szerzej – do nowych technologii komunikacyjno-informacyjnych);
- stosowaniu tzw. „miękkiego prawa", czyli zaleceń i rekomendacji, które wyznaczają kierunki działania, ale nie mają mocy prawnej i wymagają rozwiązań o charakterze samoregulacji i współregulacji dostawców treści w celu realizacji promowanych zasad.

b) Internet: zastosowanie prawa ogólnego

Unia Europejska

Przykładem rozciągnięcia prawa ogólnego (w tym przypadku wspólnotowego) na zawartość Internetu, a ściślej rzecz biorąc na audiowizualną zawartość tego medium jest przygotowywana nowelizacja dyrektywy o telewizji bez granic. Rozszerzy ona swój zakres na

wszystkie media elektroniczne poprzez zastosowanie technologicznie neutralnej, stopniowalnej regulacji zawartości audiowizualnej, z dużym udziałem samo- i współregulacji w odniesieniu do treści przekazywanych przez Internet, do których nie można zastosować tradycyjnego modelu regulacji. Przedmiotem tej regulacji nie będą wszystkie treści dostępne w Internecie, a tylko „audiowizualne usługi medialne" w postaci programów telewizyjnych lub form „Video on Demand" dystrybuowanych za pośrednictwem Internetu.

Rada Europy

Z kolei, Deklaracja Komitetu Ministrów Rady Europy w sprawie swobody komunikowania w Internecie (2003) jest przykładem użycia „miękkiego instrumentu", który nie ma mocy prawnej, lecz wskazuje pewien kierunek myślenia i wyznacza kierunek postępowania dla państw członkowskich tej organizacji. Przykład ten ilustruje postulat traktowania tego medium na zasadach ogólnych, czyli na tych samych zasadach, co inne formy dostarczania zawartości. Deklaracja stwierdza między innymi, że państwa członkowskie Rady Europy nie powinny poddawać treści internetowych bardziej surowej regulacji aniżeli tej odnoszącej się do innych form dostarczania treści i nie powinny wprowadzać systemów zezwoleń lub koncesji (np. na założenie witryny internetowej) opartych wyłącznie na wykorzystywanej w Internecie technologii upowszechniania informacji, czy też wprowadzać filtry bądź inne formy blokowania dostępu do treści (chyba, że w celu ochrony małoletnich lub godności ludzkiej). Państwa członkowskie powinny natomiast wspierać dostęp do Internetu oraz samo- lub współregulację zawartości rozpowszechnianej przez Internet. Zgodnie z Deklaracją, państwa nie powinny wprowadzać ogólnego obowiązku monitorowania treści przez dostawców usług internetowych. W przypadku gdy ich funkcje są szersze i przechowują oni treści dostarczane przez osoby trzecie, a nie podejmują kroków niezbędnych do usunięcia treści szkodliwych lub nielegalnych, państwo może obciążyć ich współodpowiedzialnością za rozpowszechnianie takich treści.

Powyższa Deklaracja wyraźnie opowiada się za nie tworzeniem regulacji prawnych przeznaczonych specjalnie dla Internetu, lecz za traktowaniem go na poziomie prawa na zasadach ogólnych. Jednocześnie, Deklaracja wskazuje na samo- i współregulację zawartości jako metodę realizowania polityki państw członkowskich w tym zakresie.

c) Regulacje prawne stworzone specjalnie dla Internetu

Rada Europy

Oprócz wyżej wymienionej Deklaracji postulującej traktowanie Internetu na zasadach ogólnych, ta sama organizacja ma na jednak na swoim koncie instrument prawny przeznaczony specjalnie dla tego medium. Chodzi o Konwencję o cybersprzestępczości (2001) oraz Dodatkowy Protokół do tej Konwencji dotyczący ścigania aktów rasistowskich i ksenofobicznych popełnionych za pomocą systemów komputerowych (2002).

Konwencja wprowadza równowagę między prawami człowieka a ochroną przed treściami nadużywającymi tych praw. Jej celem jest zagwarantowanie bezpieczeństwa sieci i jej użytkowników. Tworzy ramy prawne do zwalczania m.in. pornografii dziecięcej (art. 9) oraz treści rasistowskich i ksenofobicznych w Internecie, zawiera przepisy dotyczące odpowiedzialności państw-stron konwencji za przestępstwa popełnione na ich terenie, określa środki, jakie należy podjąć na szczeblu krajowym w zakresie prawa karnego materialnego, prawa procesowego i kwestii jurysdykcyjnych, a także tworzy podstawy systemu skutecznej i szybkiej współpracy międzynarodowej. Jeśli chodzi o współpracę międzynarodową, Konwencja określa jej zasady ogólne (dotyczące ekstradycji, zasady wzajemnej pomocy prawnej, procedury przy braku obowiązujących porozumień międzynarodowych itp.) oraz szczegółowe (wzajemna pomoc prawna w zakresie środków tymczasowych i odnosząca się do środków śledczych, wyznaczenie sieci punktów kontaktowych działających 24 godziny na dobę przez 7 dni w tygodniu). Konwencja harmonizuje ponadto prawodawstwa krajowe w zakresie terminologii, na przykład oprócz definicji systemu informatycznego czy danych informatycznych, definiuje też dostawców usług i danych w Internecie.

W opracowanie Konwencji o cyberprzestępczości zaangażowanych było 48 krajów, w tym 44 państwa członkowskie oraz 4 tak zwane kraje partnerskie (Kanada, USA, Japonia i Afryka Południowa), co nadaje jej szerokiego międzynarodowego wymiaru. Mimo silnego zaangażowania w jej opracowanie, proces jej podpisywania i ratyfikacji jest stosunkowo powolny: od momentu otwarcia do podpisu w listopadzie 2001 r. sygnatariuszami Konwencji (bez ratyfikacji) jest 31 krajów, w tym wszystkie 4 kraje partnerskie (stan na październik 2005 r.). Ratyfikowało ją natomiast 11 następujących krajów: Albania, Bułgaria, Chorwacja, Cypr, Dania, Estonia, Węgry, Litwa, Rumunia, Słowenia oraz Macedonia, czyli w przeważającej większości - postkomunistyczne kraje o rozwijającej się gospodarce. Praktyczna nieobecność w tym gronie znaczących krajów o utrwalonych tradycjach demokratycznych i rozwiniętej

gospodarce może świadczyć o funkcjonującej w nich silnej przeciwwadze tendencji prorynkowych i wolnościowych lub przeciwnie - o posiadaniu przez nie na tyle rozwiniętych wewnętrznych systemów samo- i współregulacyjnych, że osłabia to ich motywację do szybkiego podpisania / ratyfikacji Konwencji. Inny z możliwych powodów takiej postawy ze strony licznych państw wysoko rozwiniętych to dylemat dotyczący granic suwerenności poszczególnych państw (patrz też punkt 5. b).

Dodatkowy Protokół do Konwencji zobowiązuje do ścigania treści o charakterze rasistowskim lub ksenofobicznym rozpowszechnianych w Internecie, uznając je tym samym za sprzeczne z prawem. Został on przyjęty przez Komitet Ministrów Rady Europy w listopadzie 2002 r. a w styczniu 2003 r. nastąpiło jego otwarcie do podpisu. Dotychczas podpisało go (bez ratyfikacji) 25 krajów, a ratyfikowały 4 (stan na październik 2005 r.). Protokół ten, oprócz harmonizacji prawa karnego, nakierowany jest na poprawę współpracy międzynarodowej w celu skuteczniejszego zwalczania rasizmu i ksenofobii w Internecie.

Unia Europejska

Unia Europejska również posługuje się instrumentami stworzonymi specjalnie dla Internetu (choć w tym przypadku rozciąga zakres zastosowania także na inne nowe technologie sieciowe). Do instrumentów tych należą Decyzje powołujące dwa kolejne programy pomocowe skierowane do państw członkowskich w ramach promocji bezpiecznego korzystania z Internetu. Chodzi o Program *Safer Internet Action Plan* (SIAP) [22] na lata 1999 – 2002/2004 z budżetem ponad 38 mln. euro oraz jego kontynuację w postaci najnowszego Programu *Safer Internet Plus* na lata 2005-2008 z budżetem 45 mln. euro [23].

Safer Internet Action Plan (SIAP)

U podstaw utworzenia Programu *Safer Internet Action Plan* leżało występowanie nielegalnych oraz szkodliwych treści w Internecie. Program dostarczał fundusze na zwalczanie niebezpiecznej zawartości stron internetowych przy pomocy środków zachęty wobec dostawców treści i usług do wdrażania rozwiązań samoregulacyjnych oraz systemów filtrowania i ratingu (oceniania). W praktyce oznaczało to brak poparcia dla wszelkich

[22] Więcej informacji o Programie patrz www.saferinternet.org

[23] Decyzja nr 854/2005WE Parlamentu Europejskiego i Rady z dnia 11 maja 2005 r. w sprawie ustanowienia wieloletniego programu wspólnotowego na rzecz promowania bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych.

zdecydowanych rozwiązań regulacyjnych ze strony państw członkowskich. Szczegóły na temat struktury Programu, jego celów i ich realizacji zawiera Załącznik nr 2.

Ewolucja w postawie Unii Europejskiej

Wracając do jednego z głównych wątków debaty dotyczącego zakresu i przesłanek ograniczania swobody komunikowania w Internecie, sama Unia Europejska nie jest wolna od wewnętrznej debaty i ewolucji swojego stanowiska w tym zakresie. Ewolucję jej postawy w zakresie dążenia do równowagi między swobodą komunikowania w Internecie a innymi prawami i swobodami obywatelskimi ilustruje prześledzenie aktywności tej organizacji w odniesieniu do treści sprzecznych z prawem i potencjalnie szkodliwych. Pierwsze działania przeciw treściom nielegalnym podjęła Rada Unii Europejskiej w lipcu 1996 r. Uczyniła to w oparciu o artykuł K.3 Traktatu w Maastricht, przyjmując plan walki z rasizmem i ksenofobią. Następnie, w 1997 roku Rada ds. Telekomunikacji przyjęła rezolucję w sprawie szkodliwych lub nielegalnych treści w Internecie. 16 października 1996 roku Komisja Europejska wydała oświadczenie pt. „Nielegalne i szkodliwe treści w Internecie", w którym podkreślono „wysoce zdecentralizowaną i transnarodową naturę Internetu" oraz rekomendowano „skoordynowaną reakcję na międzynarodowym i europejskim szczeblu".

Komisja odrzucała wówczas wszelki system kontroli oparty na blokowaniu dostępu połączony z utworzeniem czarnej listy miejsc i stron, uznając, że „tego typu restrykcyjny system jest nie do przyjęcia w Europie, bowiem poważnie naruszyłby wolność jednostek i tradycje polityczne", a ponadto byłby przeciwny zasadzie wolnego handlu, która rządzi prawnymi ramami rynku. Stwierdzała natomiast, że jest za użyciem filtrującego oprogramowania instalowanego na komputerach użytkowników, umożliwiającego nadzór rodzicielski, jako rozwiązania pragmatycznego, zapewniającego poszanowanie różnych form wrażliwości rodzinnej i narodowej, bez szkody dla wolnego przepływu informacji. Zachęcając dostawców treści i oprogramowania „do formowania wspólnej platformy dla użycia systemów filtrujących w ramach Unii", Komisja zachęcała europejskich dostawców usług do przyjęcia ich własnych kodeksów etycznych i prosiła dostawców Internetu o rozpoczęcie procesu samoregulacji poprzez ustanawianie „sygnalizujących" procedur za pomocą linii telefonicznych (*Hotlines*), co zostało rozwinięte w Programie *Safer Internet Action Plan*.

W trakcie realizacji Programu okazało się, że realizacja jego celów wymaga nie tylko kontynuacji w postaci nowej edycji, ale też wzmocnienia i przekierunkowania pewnych

działań oraz zwiększenia środków finansowych i zintensyfikowania ich wydatkowania (z 45 mln. euro przyznanych na program o nazwie *Safer Internet Plus* 20, 5 mln. euro ma przypaść na okres do końca 2006 r.). Wszystko to świadczy, iż Unia biorąc pod uwagę poziom zagrożenia godności ludzkiej i małoletnich treściami nielegalnymi i potencjalnie szkodliwymi, przykłada coraz większą wagę do bezpiecznego korzystania z Internetu. Jednocześnie, przeznaczenie blisko połowy nowego budżetu na działania uświadamiające (Działanie nr 4) wyraźnie świadczy o podtrzymaniu, a nawet zintensyfikowaniu wcześniej obranego kursu na zapobieganie treściom nielegalnym i szkodliwym, który to kurs Unia w dalszym ciągu chce realizować tzw. miękkimi środkami.

Safer Internet Plus

Nowy Program kontynuuje główny cel poprzedniej edycji, mianowicie promocję bezpiecznego korzystania z Internetu i innych nowych technologii sieciowych, ale jednocześnie poszerza jego zakres o treści niepożądane przez użytkowników, a także zwraca uwagę na celowość wyposażenia użytkowników końcowych, szczególnie rodziców, nauczycieli i dzieci, w odpowiednie narzędzia służące do realizacji powyższego celu. Konstrukcja obu Programów potwierdza, że w zakresie treści objętych ich zakresem, konieczne jest znalezienie właściwych proporcji między zabezpieczeniem wolnego przepływu informacji a gwarancjami ochrony społeczeństwa, szczególnie dzieci, przed natrętnymi formami marketingu, przemocy, pornografii, itp.

Ewolucję w polityce i podejściu Unii Europejskiej do problematyki bezpiecznego korzystania z zawartości Internetu odzwierciedla w nowym Programie to, że nie tylko zachęca on do tworzenia interwencyjnych linii „*Hotlines*", ale robi krok naprzód wskazując na obowiązek ich tworzenia w państwach członkowskich i stowarzyszonych oraz na potrzebę utrwalenia ich na poziomie krajowym w sposób umożliwiający ich przetrwanie i finansową stabilność po zakończeniu Programu. Ponadto Program kładzie dużo silniejszy akcent na jak najszerszą, bo znacznie podnoszącą szanse skuteczności wszelakich działań, współpracę międzynarodową, polegającą na obowiązku sieciowania linii „*Hotlines*", na współpracę transgraniczną, a także na wzmocnienie roli jednostek koordynujących „INHOPE" oraz Forum „Bezpieczniejszy Internet". Nowością o dużym znaczeniu jest także fakt, że Program ten zrównuje (przynajmniej na poziomie deklaracji) bezpieczeństwo użytkownika końcowego z podejściem rynkowym i technologicznym, a także dopuszcza (na razie tylko w

ograniczonym zakresie) działania wyrównujące działanie sił rynkowych w zakresie zapewnienia niezbędnych wersji językowych dla technologii filtrujących.

Ponieważ Program *Safer Internet Plus* stanowi źródło najbardziej aktualnej wykładni unijnego podejścia do problematyki bezpiecznego korzystania z Internetu, obszerny opis proponowanych w tym Programie działań zamieszczony został w Załączniku nr 3.

USA

Jeśli chodzi o praktykę poszczególnych krajów w zakresie tworzenia regulacji prawnych mających zastosowanie wyłącznie do Internetu, przykładu dostarczają wspomniane już wcześniej Stany Zjednoczone. Kraj ten, po latach realizacji polityki polegającej na programowym powstrzymywaniu się przed ingerencją państwa w Internet, dokonał spektakularnego zwrotu nie tylko z pobudek związanych z walką z terroryzmem (patrz. punkt 3.b.), ale również z powodów związanych z dostrzeganiem zagrożeń płynących z samego Internetu, szczególnie wobec nieletnich. Świadczy o tym projekt ustawy z końca czerwca 2005 r. o ochronie dzieci przed pornografią oraz o wzmocnieniu organów śledczych i innych działaniach w celu zwalczania pornografii i innych przestępstw internetowych wymierzonych w dzieci [24]. Projekt ten postuluje między innymi system weryfikacji wieku przy dostępie do stron pornograficznych oraz płaceniu za niego, a także używanie do tego celu oprogramowania certyfikowanego przez *Federal Trade Commission*. Projekt wprowadza też termin „regulowanych pornograficznych stron internetowych" (*regulated pornographic Web site)*, nakłada na nie podatek w wysokości 25% opłat pobieranych za wyświetlanie i dystrybucję pornografii oraz nadaje wyżej wymienionej Komisji kompetencje w zakresie nadzoru i weryfikacji systemu regulacji stron pornograficznych. Ponadto, projekt ten proponuje zintegrowany program ochrony dzieci, którego elementem jest powołanie Funduszu Powierniczego na rzecz Bezpieczeństwa w Internecie i Ochrony Dzieci, zasilanego z niektórych wpływów podatkowych. Powyższy przykład to efekt obecnego stanowiska Stanów Zjednoczonych w kwestii ograniczania swobody wypowiedzi i przepływu informacji w Internecie w tym kraju.

[24] *A Bill to protect children from Internet pornography and support law enforcement and other efforts to combat Internet and pornography-related crimes against children*.

Nie zawsze tak było. Wymowny jest szczególnie przykład losów projektu *Communication Decency Act (*Ustawa o Moralności Komunikacyjnej*)* z połowy lat 90-tych [25]. Była to poprawka stanowiąca formalnie część ustawy o reformie telekomunikacji, zgłoszona w celu – jak przyznawali jej autorzy – uczynienia z infostrad bezpiecznych szlaków podróżowania dla młodych obywateli. Mimo oporów i żywych protestów różnych organizacji społecznych (między innymi Amerykańskiej Unii Swobód Obywatelskich), które organizowały spektakularne akcje i kampanie (np. internetowy dzień protestu), poprawka ta została przyjęta przez obie izby Kongresu oraz w 1996 r. podpisana przez Prezydenta (wywołało to akcję ściemniania stron www w związku z uchwaleniem ustawy traktowanej jako cenzurującej Internet).

To nie zakończyło jednak sprawy. Różne grupy przeciwników przyłączyły się do Amerykańskiej Unii Swobód Obywatelskich i złożyły pozew do sądu przeciw wprowadzeniu nowej regulacji. Doprowadziło to ostatecznie do jej unieważnienia przez Sąd Najwyższy, a uzasadnienie powoływało się na sprzeczność z konstytucyjną zasadą wolności słowa (wypowiedzi). Internet uznano wówczas za rodzaj prasy, a nie za środek równoważny radiu i telewizji, dla których przyjmuje się w USA bardziej rygorystyczne zasady dotyczące rozpowszechniania materiałów „nieobyczajnych lub nieprzyzwoitych". W uzasadnieniu sędzia dowodził, że „rząd nie może ograniczyć dorosłym dostępu do tych tylko materiałów, które są odpowiednie dla dzieci". Z dzisiejszego punktu widzenia argumentacja ta staje się bezzasadna: świadczy o tym coraz powszechniejsza świadomość dorosłych na temat zagrożeń jakie nielegalne lub szkodliwe treści niosą małoletnim użytkownikom, a przesądza dostępność rozwiązań technicznych, których zadaniem jest blokada na życzenie rodziców lub opiekunów treści niepożądanych wyłącznie dla dzieci.

Hiszpania i Niemcy

Inne przykłady tworzenia regulacji prawnych specjalnie dla Internetu to przykład Hiszpanii, gdzie określono „Dekalog" zasad w zakresie ochrony małoletnich i zwalczania niepożądanych treści w Internecie, a także utworzono Agencję na rzecz Jakości Internetu, której celem jest nadzór nad przestrzeganiem tych zasad przez dostawców usług i treści internetowych.

[25] Źródło informacji na ten temat: Janusz Barta, Ryszard Markiewicz, Internet a prawo, Universitas, Kraków, 1998 r.

Kolejny przykład to Niemcy, gdzie usługi internetowe jako wchodzące w zakres teleusług o charakterze indywidualnym reguluje przyjęta na szczeblu federalnym ustawa *Informations-und Kommunikationsdienste-Gesetz*, a od kwietnia 2003 r. funkcjonuje tam traktat na rzecz ochrony małoletnich i godności ludzkiej w mediach (*Jugendmedienschutz-Staatsvertrag, JMStV*). Odnosi się on do wszystkich elektronicznych mediów komunikacyjnych i informacyjnych, (radio, telewizja i Internet) a zawarły go między sobą kraje związkowe. Traktat ten tworzy jednolity system wraz z jednocześnie przyjętą federalną ustawą o ochronie małoletnich (*Jugendschutzgesetz*) odnoszącą się do prasy, kaset magnetowidowych, DVD, gier itp.

Australia i Francja

Kolejnego przykładu regulacji prawnych stworzonych specjalnie dla Internetu dostarcza Australia, której rząd i parlament już od połowy lat 90-tych XX w. wykazywały aktywność w dziedzinie rozpoznawania zagrożeń i szukania rozwiązań związanych z zawartością Internetu. Pochodzący z 1996 r. raport organu regulacyjnego ds. radia i telewizji (*Australian Broadcasting Autority)* rekomendował australijskiemu rządowi szczególne podejście w zakresie nielegalnej i szkodliwej zawartości przekazywanej w Internecie w stosunku do nieletnich. Z raportu tego wynikały 3 następujące wnioski:

- potrzeba utworzenia kodeksów dobrej praktyki dla dostawców usług;
- potrzeba powołania zespołu operacyjnego do rozważenia roli systemów etykietowania zawartości (*content labelling scheme*) w celu ochrony małoletnich w środowisku internetowym;
- potrzeba wypracowania strategii edukacji społeczeństwa w celu wyciągnięcia maksymalnie dużych korzyści wynikających z użytkowania Internetu.

Jeśli chodzi o zmiany legislacyjne, polegały one na rozciągnięciu na Internet zasad obowiązujących w radiofonii i telewizji, zwłaszcza w odniesieniu do zawartości nielegalnej lub szkodliwej dla nieletnich. W tym celu, w 1999 r. znowelizowano ustawę o radiofonii i telewizji wprowadzając podstawy prawne dla systemu samo- i współregulacji zawartości przekazywanej w Internecie (*Broadcasting Services Amendment (Online Services) Bill)*. Szczególna rola w zakresie współregulacji przypadła wyżej wymienionemu organowi regulacyjnemu, który od lipca 2005 r. wchodzi w skład konwergentnego organu o nazwie

Australian Communications and Media Authority (ACMA), odpowiedzialnego za regulację telekomunikacji, radia i telewizji oraz zawartości internetowej [26].

Rola australijskiego organu regulacyjnego w odniesieniu do zawartości Internetu polega na:

- udziale w wyżej wymienionym systemie współregulacji (szerzej na ten temat poniżej);
- działaniach zachęcających przemysł internetowy do tworzenia kodeksów dobrej praktyki, a po ich stworzeniu – rejestracji tychże kodeksów [27] i monitoringu ich realizacji (szerzej na ten temat patrz punkt 4.e.);
- poradnictwie i informowaniu społeczeństwa w zakresie bezpieczeństwa Internetu, zwłaszcza w odniesieniu do korzystających z sieci nieletnich;
- podejmowaniu działań badawczo-rozwojowych w zakresie problematyki Internetu oraz na informacyjnym wsparciu dla ministra na temat nowych trendów w zakresie Internetu;
- utrzymywaniu kontaktu z odpowiednimi zagranicznymi instytucjami /organami.

W systemie współregulacji kluczowym elementem jest działający od stycznia 2000 r. system rozpatrywania skarg na zawartość Internetu (*co-regulatory scheme for Internet content*), którym objęte są treści nielegalne i szkodliwe przekazywane przez Internet. W systemie tym wyraźnie określa się jakie treści wchodzą w jego zakres, czyli tworzą *content* (są to wszystkie strony www, fora internetowe i pliki, które można ściągać za pomocą oprogramowania *peer-to-peer*), a jakie są z niego wykluczone (zwykłe wiadomości e-mailowe oraz zawartość, do której użytkownik ma dostęp w czasie rzeczywistym, na przykład czaty, przekazy głosowe lub strumieniowe treści audio i video).

Zgodnie z australijską ustawą o radiofonii i telewizji, do treści niepożądanych należy:

- zawartość Internetu zaklasyfikowana do tej kategorii przez specjalnie ciało, tzw. Narodową Radę Klasyfikacyjną (*National Classification Bard)* [28]. Są to treści

[26] Oprócz zawartości Internetu, ACMA posiada też kompetencje w zakresie spamu (patrz. *Spam Act 2003*) oraz gier komputerowych (*gambling services*).

[27] Rejestracja taka miała miejsce w maju 2005 r. i odnosiła się do *Codes for industry co-regulation in areas of Internet and mobile content.*

[28] Na podstawie odpowiednich wytycznych *National Classification Board* nadaje niepożądanym treściom specjalne oznaczenia typu RC (należą do nich treści zawierające szczegółowe instrukcje dokonywania przestępstw, używania przemocy lub używania narkotyków) oraz X, czyli realistyczne opisy nie symulowanych aktów seksualnych).

ukazujące nie symulowane akty seksualne, pornografia dziecięca, treści ukazujące okrucieństwo lub nadmierną przemoc, w tym przemoc seksualną;

- zawartość hostowana w Australii, której nie obejmuje system ograniczonego dostępu, a którą zaklasyfikowała do tej kategorii ww. Rada Klasyfikacyjna. Są to treści ukazujące symulowane akty seksualne, treści nacechowane silną, realistyczną przemocą oraz inne treści przesycone tematyką dla dorosłych.

Jeżeli niepożądana zawartość pochodzi ze źródła australijskiego, organ regulacyjny ma prawo zakazać jej dostarczania i zażądać od dostawców usług hostingowych (*Internet Content Hosts - ICH)* usunięcia z Internetu. Jeżeli zaś pochodzi ona ze źródła zagranicznego, organ ten ma obowiązek poinformowania policji oraz może wydać australijskiemu dostawcy usług (*Internet Services Providers - ISP)* zakaz przekazywania tych treści zgodnie z procedurą określoną w kodeksach dobrej praktyki. Jednocześnie, organ ten, jak też *ICH i ISP* nie zostali zobowiązani do aktywnego monitorowania Internetu i samodzielnego poszukiwania czy klasyfikowania zakazanych treści. Ponadto, wg. ustawy wykroczenia nie stanowi samo hostowanie niepożądanych treści, natomiast może się nim stać nie dostosowanie się do nakazu zdjęcia danych treści (dotyczy to nie tylko treści niepożądanych, ale również uznanych za potencjalnie niepożadane). Zresztą, każde nie wykonanie przez *ICH lub ISP* polecenia organu regulacyjnego lub nie dostosowanie się przez nich do procedur określonych w kodeksach dobrej praktyki zagrożone jest karą wysokiej grzywny, oczywiście przy zagwarantowaniu odpowiedniej procedury odwoławczej.

Ponadto, na początku 2006 r. w Australii wejdą w życie przepisy delegalizujące używanie Internetu do promowania samobójstw [29], co uczyni ten kraj pionierem w delegalizacji zawartości Internetu, którą dotychczas uznawano za szkodliwą, ale nie nielegalną.

O ile w Australii, kwestia odpowiedzialności za niepożądane treści jest jednoznacznie przypisana *ICH* oraz *ISP,* o tyle w innych krajach nie jest to tak jednoznaczne. Przykładem ilustrującym trudności w tej kwestii, na które nakładają się dodatkowo problemy jurysdykcyjne jest przykład sprawy, która miała miejsce w połowie 2005 r. we Francji i stanowiła precedens w historii Internetu w tym kraju.

W czerwcu 2005 r. Sąd w Paryżu (*Tribunal de grande instance de Paris*) nakazał 10 francuskim dostawcom dostępu do Internetu zablokowanie z terytorium francuskiego dostępu do amerykańskiego serwisu rewizjonistycznego AAARGH. Uczynił to w wyniku skargi 8

[29] Źródło: http://news.com.com/2100-1030_3-5760586.html

francuskich organizacji antyrasistowskich i powołując się na moc nowej, francuskiej ustawy na rzecz zaufania do gospodarki cyfrowej. Wyrok ten poprzedzony był nakazem tego samego sądu wydanym 2 miesiące wcześniej wobec 3 firm z siedzibą w USA, dostarczającym usługi hostingowe dla powyższego serwisu rewizjonistycznego. Francuski sąd nakazał wtedy firmom amerykańskim zamknąć na terytorium francuskim dostęp do wyżej wymienionego serwisu (nakazu usłuchały dwie z trzech firm) oraz dodatkowo przekazać stronie francuskiej dane dotyczące dostawcy treści w tym serwisie, które umożliwiłyby jego pełną identyfikację. Sąd zastrzegł wówczas, że w przypadku odrzucenia francuskiego nakazu przez amerykańskie firmy, nakaz ten zostanie w następnej kolejności skierowany do francuskich dostawców dostępu, co rzeczywiście nastąpiło w czerwcu 2005 r. Przy okazji, sytuacja ta sprowokowała ożywienie w tym kraju debaty na temat zakresu odpowiedzialności dostawców dostępu do Internetu. Na czoło tej debaty wysunął się postulat o nie czynienie dostawców dostępu jedynym podmiotem regulacji Internetu. Innymi słowy, chodzi o zapobieżenie transferu odpowiedzialności z wydawców i dostawców nielegalnych treści na dostawców dostępu. Dodatkowo, przy okazji powyższej sprawy, francuscy dostawcy dostępu nagłośnili kwestię trudności technicznych i rodzącego się konfliktu w stosunku do obowiązującego ich wymogu neutralności, a francuskie środowisko internetowe uznało wyżej opisaną decyzję sądu za otwarcie puszki Pandory.

d) „Miękkie prawo" odnoszące się do Internetu (wyznacza kierunki działania, lecz nie posiada mocy prawnej)

Na tym poziomie relacji prawo - Internet znajdują się wszelkie działania samoregulacyjne jak też Zalecenia, Rekomendacje oraz inicjatywy i propozycje rozwiązań dla państw członkowskich Unii Europejskiej czy Rady Europy.

Unia Europejska

Do regulacji tego typu należy Zalecenie Parlamentu Europejskiego i Rady 98/560/WE z dnia 24 września 1998 r. w sprawie rozwoju konkurencyjności europejskiego przemysłu usług audiowizualnych i informacyjnych poprzez wspieranie ram krajowych mających na celu osiągniecie porównywalnego i efektywnego poziomu ochrony nieletnich i godności ludzkiej. Zalecenie to stanowi pierwszy unijny instrument prawny w zakresie zawartości usług audiowizualnych i informacyjnych *online* oraz rozpowszechnianych w Internecie.

Stanowi ono akt prawny przewidziany przez art. 249 (ex-189) Traktatu ustanawiającego Wspólnotę Europejską i służy wskazaniu kierunków legislacji krajowych dla państw członkowskich. Zalecenie to obejmuje media elektroniczne w całości. Zachęca operatorów internetowych do wypracowania kodeksów dobrej praktyki w celu skuteczniejszej realizacji i doprecyzowania aktualnych ustawodawstw krajowych. Zalecenie wskazuje też kierunki działania dla rozwoju krajowych samoregulacji w zakresie ochrony małoletnich i godności ludzkiej w oparciu o 3 następujące podstawy:

- współuczestnictwo wszystkich stron (władze, przemysł, dostawcy dostępu oraz stowarzyszenia użytkowników) w wypracowaniu kodeksów dobrej praktyki;
- wcielenie w życie wypracowanych kodeksów przez przemysł internetowy;
- ewaluacja ww. działań.

Zakres powyższego Zalecenia zostanie rozszerzony (uwzględniając efekty procesu konwergencji) i uzupełniony przez nowe Zalecenie Parlamentu Europejskiego i Rady w sprawie ochrony nieletnich i godności ludzkiej oraz prawa do odpowiedzi w związku z konkurencyjnością europejskiego przemysłu usług audiowizualnych i informacyjnych *on-line* (projekt z 30 kwietnia 2004 r.). Dokument ten z poprawkami został przyjęty przez Parlament Europejski podczas pierwszego czytania we wrześniu 2005 r. Zaleca on państwom członkowskim zachęcanie przemysłu usług informacyjnych *online* do unikania i zwalczania dyskryminacji na tle rasowym, etnicznym, religijnym i wyznaniowym, a także na tle płci, niepełnosprawności, wieku lub orientacji seksualnej, jak również do tworzenia warunków do bezpiecznego korzystania z Internetu oraz do zapewniania dostępu do usług wysokiej jakości. Nowym elementem projektu tego Zalecenia jest ponadto zachęta ze strony Komisji do „współpracy i przekazywania doświadczeń pomiędzy organami (samo)regulującymi, które zajmują się oceną lub klasyfikacją treści w celu umożliwienia wszystkim użytkownikom, w szczególności rodzicom i nauczycielom oceny treści usług audiowizualnych i informacyjnych online". Unijnym sprawozdawcą tego projektu jest francuska eurodeputowana, Marielle de Sarnez, która we wrześniu 2005 r. przedstawiła raport w zakresie ochrony dzieci i godności ludzkiej przed szkodliwą zawartością Internetu. W oparciu o ten raport, Parlament Europejski domaga się, między innymi, utworzenia specjalnej kategorii domen internetowych o charakterystycznym rozszerzeniu *"kid",* a także wprowadzenia technicznych rozwiązań. uniemożliwiających dostęp do treści szkodliwych dla dzieci bez zgody rodziców. Postawę swa eurodeputowani uzasadniają twierdząc, że "dziś nie wystarczą już tylko etyczne kodeksy postępowania. Najwyższy czas, by dostawcy usług i treści internetowych zapewnili rodzicom

proste w użyciu oprogramowanie, automatycznie filtrujące treści pornograficzne, rasistowskie czy zawierające przemoc". Parlament Europejski chce też, by Komisja Europejska utworzyła specjalną infolinię telefoniczną, przez którą udzielana byłaby informacja dla rodziców, opiekunów i wychowawców o tym, jak radzić sobie z niepożądanymi materiałami w Internecie, w tym na przykład jak filtrować zawartość witryn internetowych. Chcą też, by możliwość zgłaszania skargi na treści zawarte w prasie czy telewizji rozszerzona została na nowe media elektroniczne, takie jak właśnie Internet [30].

Rada Europy

Instrumentami z zakresu „miękkiego prawa" posługuje się również Rada Europy. W ramach działań na rzecz bezpiecznego korzystania z Internetu wydała ona dwie następujące Rekomendacje:

- Rekomendacja Komitetu Ministrów Rec(2001)16 w sprawie ochrony dzieci przed seksualnym wykorzystywaniem (2001);
- Rekomendacja Komitetu Ministrów Rec(2001)8 dotycząca samoregulacji w zakresie cyber-zawartości: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych (2001).

Obie Rekomendacje pełnią rolę instrumentów politycznych (wskazują polityczne zaangażowanie państw członkowskich), a nie prawnych (nie mają mocy prawnej), są skierowane do rządów państw członkowskich, którym wskazują konkretne cele do osiągnięcia w zakresie przyczynienia się do bezpiecznego korzystania z Internetu, pozostawiając im jednocześnie swobodę w doborze sposobów realizacji zgodnie z krajowymi prawodawstawami i praktykami oraz międzynarodowymi zobowiązaniami i narodową specyfiką.

Rekomendacja w sprawie ochrony dzieci przed seksualnym wykorzystywaniem poświęca Internetowi cały oddzielny punkt (część II, punkt e). Więcej informacji na ten temat znajduje się w Załącznik nr 4.

Jeśli chodzi o Rekomendację w sprawie cyber-przestępczości, wiele elementów przez nią zalecanych pokrywa się z rozwiązaniami proponowanymi przez Unię Europejską, a wśród nowych propozycji znajdują się między innymi opisy zawartości, narzędzia dostępu warunkowego, czy system mediacji i arbitrażu. Rekomendacja ta, kierując się do państw członkowskich, określa

[30] Źródło: http://wirtualnemedia.pl/document.php?id=332377

ich rolę w zakresie promocji bezpiecznego korzystania z Internetu, formułując przy okazji oczekiwania Rady Europy wobec dostawców treści i usług internetowych, jak też samych użytkowników Internetu. Podobnie jak w rozwiązaniach proponowanych przez Unię Europejską ukazana w Rekomendacji rola poszczególnych państw nie jest rolą sprawczą czy silnie ingerującą. Jest to rola ograniczona do zachęcania i tworzenia właściwych warunków do działań, których realizacja należy do środowiska internetowego (szczegóły - patrz Załącznik nr 4).

e) Samoregulacja

Organizacje samoregulacyjne

W Europie działają takie organizacje samoregulacyjne jak:

- EuroISPA (grupuje dostawców usług internetowych);
- INHOPE (grupuje organizatorów linii interwencyjnych „Hotlines" takich jak polski Dyżurnet);
- INCORE (tworzy system opisu zawartości internetowej w celu odsiewania treści nielegalnych lub szkodliwych);
- ICRA (dokonuje oceny i „etykietowania" zawartości internetowej, aby użytkownicy wiedzieli z czym mają do czynienia);
- Sieć EICN (*European Internet Coregulation Network* - promuje współpregulację, czyli współpracę między państwem a podmiotami rynkowymi w celu osiągania wspólnych celów). Do sieci tej należą następujące narodowe i międzynarodowe organizacje:
  - ✓ Forum pour la Tecnologia della Informazione (Włochy);
  - ✓ Institute Rattsinformatik (Szwecja);
  - ✓ Internet Watch Foundation (Wielka Brytania)
  - ✓ Oxford Internet Institute (Wielka Brytania);
  - ✓ Informacios Tarsadalom-esTrendkutato Kozpont (Węgry);
  - ✓ Observatoire des droits de l'internet - Observatorium van de Rechten op het
  - ✓ Internet (Belgia);
  - ✓ Österreichisches Institut für angewandte Telekommunikation (Austria);
  - ✓ Le Forum des droits sur l'Internet (Francja);
  - ✓ Confederation of European Komputer User Associations - CUA

Wszystkie powyżej wymienione organizacje samoregulacyjne cieszą się wsparciem i pomocą Unii Europejskiej w ramach opisanego w Załączniku nr 2 Programu *Safer Internet Action Plan.*

Internet Watch Fundation

Jedną z najbardziej znanych i prężnych organizacji samoregulacyjnych jest brytyjska fundacja *Internet Watch Foundation (IWF*). Do powołania jej doprowadziło wspólne działanie dostawców usług internetowych, stowarzyszeń zawodowych (np. London Internet Exchange) oraz policji z poparciem rządu angielskiego. Fundacja finansowana jest przez instytucje prywatne. Jej główne cele obejmują:

- zapobieganie rozpowszechnianiu w Internecie nielegalnych treści;
- dostarczanie użytkownikom programów i narzędzi ochrony ich samych i ich dzieci przed szkodliwymi treściami i kontaktami w Internecie.

  Działanie Internet Watch Foundation opiera się na trzech następujących filarach:

- procedurze zawiadamiania i "zdejmowania" zabronionych treści;
- etykietowaniu i filtrowaniu treści potencjalnie szkodliwych;
- podejmowania inicjatyw uświadamiających i edukacyjnych w celu zmierzenia się z problemem bezpieczeństwa w sieci.

System zawiadamiania i "zdejmowania nielegalnych treści" działa w oparciu o zasadę, że jeżeli dostawcy usług internetowych (ISP) będą powiadamiani o istnieniu takich treści na swoich serwerach, to będą je usuwać. Linia interwencyjna IWF (*Hotline*) zajmuje się zatem odbieraniem od społeczeństwa zawiadomień o istnieniu takich treści, wchodzeniem na strony, na których się one znajdują, ocenianiem ich szkodliwości oraz przekazywaniem dostawcom informacji, czy dane treści zostały uznane za potencjalnie nielegalne. Hotline IWF informuje również o danym zgłoszeniu organy prawa, a także - w przypadku treści pochodzących spoza Wielkiej Brytanii, tam gdzie jest to możliwe, przekazuje informacje na ten temat do linii interwencyjnej kraju pochodzenia tych treści.

W swoich działaniach, IWF w dużej mierze opiera się na pracy reprezentatywnego ciała konsultacyjnego, w którego skład wchodzą zarówno przedstawiciele różnych organizacji branżowych, jak też rządu, policji i rad medialnych.

Jednym z głównych postulatów IWF jest pilna potrzeba ścisłej współpracy międzynarodowej, gdyż mimo prężnego działania tej organizacji wobec treści nielegalnych wywodzących się z Wielkiej Brytanii, okazuje się, że większość tego typu treści pochodzi jednak spoza tego kraju.

Kodeksy dobrej praktyki / kodeksy postępowania

Jednym z podstawowych narzędzi używanych w ramach samoregulacji są kodeksy dobrej praktyki / kodeksy postępowania opracowywane przez sam przemysł internetowy i zatwierdzane (lub jak w przypadku Australii również rejestrowane) przez właściwy organ regulacyjny, który również monitoruje ich przestrzeganie. Kodeksy te zawierają zbiory reguł i procedur stosowanych przez dostawców usług internetowych. Duży nacisk kładzie się przy tym na wypracowanie procedur związanych z usuwaniem materiałów nielegalnych z sieci w przypadku hostingu. Warto przy okazji przypomnieć, że zarówno Rekomendacja Rady Europy o cyber-zawartości (szczegóły: patrz Załącznik nr 4) jak i dyrektywy unijne nie przewidują obowiązku tworzenia tych kodeksów. Na przykład, Dyrektywa 2000/31/WE o handlu elektronicznym mówi tylko o wspieraniu ich opracowywania. Mają one bowiem przyczynić się do sprawnej realizacji innych postanowień dyrektywy, zwłaszcza tych, które dotyczą odpowiedzialności prawnej dostawców usług internetowych za materiały umieszczane w sieci przez osoby trzecie.

Przykładem takich kodeksów są australijskie *Codes for industry co-regulation in areas of Internet and mobile kontent.* Zostały one opracowane przez krajowe stowarzyszenie o nazwie *Internet Industry Association* na podstawie wymagań zawartych w znowelizowanej w 1999 r. ustawie *Broadcasting Services Act*. Ich rejestracja przez organ regulacyjny miała miejsce w maju 2005 r. Kodeksy te w szczegółowy sposób regulują obowiązki australijskich dostawców usług internetowych w zakresie hostowania zawartości Internetu na terytorium Australii oraz w zakresie dostarczania dostępu do zawartości Internetu pochodzącej zarówno z Australii jak i spoza niej.

5. PROBLEMY JURYSDYKCYJNE I TRUDNOŚCI Z PRZYPISANIEM ODPOWIEDZIALNOSCI W ZAKRESIE NADUŻYĆ SWOBODY WYPOWIEDZI I INFORMACJI W INTERNECIE

Poszczególne kraje w różny sposób radzą sobie z nadużyciami swobody wypowiedzi i informacji w Internecie. Najczęściej czynią to metodą prób i błędów. Szczególnych trudności dostarcza kwestia jurysdykcji sądów narodowych w sprawach dotyczących cyberprzestrzeni. Trudności te związane są z transgranicznością Internetu oraz z różnymi systemami prawa w poszczególnych krajach, a także – w przypadku zapadnięcia orzeczenia – z międzynarodową nieskutecznością krajowych orzeczeń.

Różnorodność krajowych sytuacji regulacyjnych jest szeroka. Z jednej strony, w wielu krajach w ogóle nie ma regulacji dotyczących aktywności internetowej, z drugiej takie kraje jak Australia, Francja, Niemcy oraz Włochy dysponują regulacjami umożliwiającymi pociągnięcie do odpowiedzialności w związku z istnieniem danej zawartości w sieci niezależnie od tego, gdzie takie treści zostały opublikowane. Również Wielka Brytania ma już doświadczenia związane z odpowiedzialnością za materiały publikowane w sposób transgraniczny [31]. Kluczową kwestią w takich sprawach staje się odpowiedź na następujące pytania: komu i w zakresie jakich obszarów należy przypisać odpowiedzialność odnośnie funkcjonowania w Internecie treści nadużywających swobody wypowiedzi i informacji, a także w jaki sposób dokonuje się podziału zakresów tej odpowiedzialności [32] ?

a) Odpowiedzialność dostawców usług internetowych

Jedną z barier przestrzegania prawa w Internecie jest komercyjne nastawienie dostawców usług internetowych. Stoją oni przed dylematem polegającym z jednej strony na byciu traktowanym jako podmioty ponoszące odpowiedzialność społeczną za dostarczane usługi, z drugiej - na konieczności pomnażania zysków. Zwykle dostawcy usług bronią się przed odpowiedzialnością argumentując, że są tylko "nośnikami" (*common carriers*), które nie mogą sprawować kontroli ani nad przekazywanymi treściami, ani nad działaniami użytkowników. Przypominają również, że nie są "wydawcami" treści, a także, że nie są w stanie technicznie kontrolować ruchu w sieci. Niemożność kontroli dodatkowo wzmacniają argumentem finansowym (kontrola taka wiązałaby się ze wzrostem nakładów finansowych,

[31] Źródło: Piotr Waglowski, „Nie każdy uzna, że deszcz pada”, 14.05.2003 r., http://www.vagla.pl/felietony/felieton_005.htm

[32] Na ten temat patrz też w treści punktów 2.a), 4.c) oraz w Załączniku nr 4.

co podwyższałoby koszty dostępu do Internetu, a to z kolei jest sprzeczne z polityką Unii Europejskiej).

Problemu nie ułatwia też kwestia różnorodności nazewnictwa i definicji dostawców usług internetowych. Termin ten jest często używany w sposób ogólny, bez różnicowania pomiędzy usługą dostarczania dostępu do Internetu a usługami przechowywania (hostowania) i przekazywania treści. Jedna i ta sama firma może należeć do różnych kategorii, ale różnice między nimi precyzuje Dyrektywa 2000/31/WE z 8.06.2000 r. o handlu elektronicznym (Art.12, 13, 14) [33]. Artykuł 15 powyższej Dyrektywy wskazuje, że państwa nie mogą narzucać obowiązku „nadzorowania informacji, które przekazują lub przechowują ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność", jakkolwiek ustawodawstwo wielu krajów wprowadza obowiązek sądowy dla dostawców usług wspomagania policji, włączając tu dostarczanie danych o użytkownikach oraz ułatwiając jej nadzór sieci.

W praktyce dostawcy usług internetowych oferują kilka rodzajów usług, w tym z usługę podłączenia do Internetu. Gdyby taki dostawca na tym poprzestał, byłby on rzeczywiście jedynie dostawcą usługi dostępowej, a korzystanie z Internetu zależałoby wówczas całkowicie od użytkownika. Jednak tylko nieliczni usługodawcy ograniczają się do tak prostej usługi. Większość z nich oferuje pocztę elektroniczną, grupy dyskusyjne, serwery www, utrzymywanie stron domowych czy serwery gier albo oprogramowanie dla chatów. W takim przypadku, w świetle powyższej dyrektywy (Artykuł 14) ich odpowiedzialność może być większa. Ona właśnie stanowi punkt odniesienia dla tworzonych w ramach samoregulacji kodeksów postępowania (kodeksów dobrej praktyki). Nad nią też czuwają instytucje prawne, a w niektórych krajach również obywatelskie.

b) Odpowiedzialność poszczególnych państw

Rada Europy

Kontrowersje pod względem jurysdykcji i odpowiedzialności poszczególnych państw wzbudza Konwencja Rady Europy o cyberprzestępczości. Być może stanowi to klucz do wytłumaczenia powolności procesu jej podpisywania, a zwłaszcza ratyfikowania przez kraje wysoko rozwinięte szczycące się silnie umocowanymi wolnościami obywatelskimi (patrz też.

[33] http://europa.eu.int/eur-lex/pl/dd/docs/2000/32000L0031-PL.doc

punkt 4.c). Jak zauważa Piotr Waglowski w artykule „Sądy właściwe i normy kolizyjne” [34] nie jest sporna ogólnie wyrażana konieczność tworzenia warunków dla międzynarodowej współpracy dotyczącej ścigania przestępstw i tworzenia spójnego systemu prawa międzynarodowego, jednak problemy pojawiają się gdy dochodzi do konkretów, na przykład w zakresie określenia granic suwerenności państw. I tak na przykład USA co prawda podpisały konwencję, ale jej nie ratyfikowały gdyż pojawiły się głosy sprzeciwu przeciwko oddaniu amerykańskich obywateli do dyspozycji zagranicznych wymiarów sprawiedliwości, co stanowiłoby problem zwłaszcza w tych krajach, w których prawa i wolności człowieka chroni się w inny sposób niż w USA. Dlaczego amerykański obywatel ma odpowiadać za coś, co w USA nie jest wykroczeniem przeciwko obowiązującemu tam systemowi prawnemu, a w innych krajach jest nielegalne ? Oto kluczowe pytanie pozostające na razie bez odpowiedzi, co nie stoi jednak na przeszkodzie w mnożeniu kolejnych dylematów prawnych związanych z transgranicznością Internetu oraz z międzynarodową nieskutecznością krajowych orzeczeń – patrz poniżej.

USA vs. Francja

Przykładem ilustrującym sytuację gdy sąd jednego kraju wydaje decyzję nieakceptowaną przez sąd drugiego kraju (problem transgraniczności Internetu i różnych systemów prawa) jest sprawa *Sarl Louis Feraud International v.Viewfinder, Inc* [35] *(*sprawa ta zahacza również o relację pomiędzy wolnością słowa a własnością intelektualną). Amerykańska firma WiewFinder została pozwana do sądu we Francji przez dwie tamtejsze firmy projektujące modę w związku z opublikowaniem w swoim serwisie internetowym projektów, co według projektantów naruszało ich prawa autorskie oraz godziło w ich marki. W 2001 r. Sąd w Paryżu przychylił się do takiego poglądu i zasądził odszkodowanie, o którego wyegzekwowanie obaj projektanci zwrócili się do sądu amerykańskiego, uznając, że amerykańska Pierwsza Poprawka do Konstytucji nie chroni nieuprawnionego publikowania grafik. W 2005 r. amerykański sąd uznał jednak francuskie orzeczenie za nieskuteczne, gdyż według niego firma działała w ramach wolności słowa gwarantowanej przez Pierwszą Poprawkę do Konstytucji, a wolność ta (jak sąd sam przyznał) może być ograniczona w innych demokratycznych krajach. Sąd stwierdził ponadto, że *obraz może zastąpić tysiące słów*

[34] Źródło: Piotr Waglowski, „Sądy właściwe i normy kolizyjne”, 22.12.2004 r., http://prawo.vagla.pl/node/4713

[35] Źródło: Piotr Waglowski, Transgraniczność i nieskuteczne francuskie wyroki, 10.10.2005 r., http://prawo.vagla.pl/node/5597

(zwłaszcza gdy opublikowany jest w serwisie mającym za zadanie przybliżyć sylwetki projektantów, i nawet wtedy, gdy serwis nie dostarcza aktualnych doniesień prasowych na temat tychże projektantów). Podstawę odmowy wykonania francuskiego orzeczenia stanowiła jego niezgodność z polityką publiczną stanu, w którym orzekał sąd amerykański [36].

Podobnego przykładu w tym zakresie dostarcza sprawa Yahoo, w której amerykański sąd odmówił wykonania francuskiego wyroku zakazującego udostępniania francuskim internautom internetowych stron, na których handlowano nazistowskimi pamiątkami [37]. W tym przypadku, amerykański sąd zastosował tę samą co powyżej podstawę odmowy wykonania orzeczenia wydanego przez sąd francuski, czyli jego niezgodność z polityką publiczną.

Australia

Jak pisze Piotr Waglowski w cytowanym już artykule „Sądy właściwe i normy kolizyjne", podczas rozpatrywania sprawy przed Sądem Najwyższym w Australii w 2001 roku przywołano precedens pochodzący z XIX w., określający międzynarodową właściwość sądu w sprawach o zniesławienie. Zgodnie z tym precedensem (i po jego uwspółcześnieniu), uznano, że publikacja internetowa powstaje w momencie, gdy dany materiał (tekst, grafika etc..) zostaje umieszczony na serwerze webowym i w tym kontekście należy ustalić właściwość sądu.

W innej sprawie, tzw. sprawie *Gutnick v. Dow Jones* [38], australijski magnat górniczy Joseph Gutnick poczuł się zniesławiony artykułem, który ukazał się w 2000 r. w serwisie internetowym Barron's, wydawanym przez amerykańskie wydawnictwo Dow Jones. Wydawnictwo twierdziło, że artykuł został opublikowany w Stanach Zjednoczonych, a J. Gutnick - że był on dostępny dla czytelników w Australii, w związku z czym pozwał wydawnictwo do sądu w tym właśnie kraju. W 2002 r. australijski sąd uznał swoją

[36] "*American courts have recognized that foreign judgments that run afoul of First Amendment values are inconsistent with our notions of what is fair and just, and conflict with the strong public policy of our State*" (orzeczenie jeszcze nie opublikowane, 2005 WL 2420525 (S.D.N.Y.). Źródło: komentarz internauty do artykułu Piotra Waglowskiego, Transgraniczność i nieskuteczne francuskie wyroki, 10.10.2005r. http://prawo.vagla.pl/node/5597

[37] Yahoo! v. La Ligue Contre le Racisme et l'Antisemitisme 169 F.Supp.2d 1181 (N.D.Cal.2001) za http://prawo.vagla.pl/node/5597

[38] Źródło: Piotr Waglowski, „Po australijskim orzeczeniu" , 11.12.2002 r. oraz „Dow Jones pozwany w Australii"10.12.2002 r., http://prawo.vagla.pl/node/1949 oraz http://prawo.vagla.pl/node/1953

miejscową właściwość dla rozstrzygania w tej sprawie. Było to pierwsze tego typu orzeczenie na świecie. Dało ono możliwość pozwania przed australijski sąd każdego wydawcy internetowego i to nawet przez podmioty, które nie muszą być w jakikolwiek sposób związane z terytorium tego kraju.

6. ZAKOŃCZENIE

Jak piszą Janusz Barta i Ryszard Markiewicz w książce pt. Internet a prawo „wśród podstawowych wolności gwarantowanych w demokratycznych krajach, swoboda wypowiedzi należy niewątpliwie do tych, które skupiają szczególną uwagę z punktu widzenia analizy i oceny funkcjonowania Internetu" [39] . Niniejsze opracowanie starało się przybliżyć przebieg i charakter debaty, która od kilku lat toczy się w tej sprawie między zwolennikami nieograniczonej swobody wypowiedzi w tym medium, a tymi, którzy dążą do jej zrównoważenia z innymi prawami i swobodami obywatelskimi. W grę wchodzi szczególnie ochrona małoletnich i godności ludzkiej przed treściami sprzecznymi z prawem oraz potencjalnie szkodliwymi, a także kwestie związane z bezpieczeństwem publicznym i jego przełożeniem na ograniczenie swobód obywatelskich, w tym swobody wypowiedzi i przepływu informacji w Internecie.

Debata ta przechodzi przez różne etapy, jest niejednorodna i otwarta, a płynące z niej doraźne wnioski nie wyczerpują tematu i siłą rzeczy nie mogą być traktowane jako ostateczne. W związku z tym, pytanie jak na gruncie prawa zapewnić równowagę między swobodą wypowiedzi zagwarantowaną w Europejskiej Konwencji Praw Człowieka (art.10) oraz Powszechnej Deklaracji Praw Człowieka (art. XIX) a innymi prawami i swobodami obywatelskimi, pozostaje nadal otwarte. Otwarte pozostaje też pytanie, czy oraz w jakim stopniu i zakresie społeczność międzynarodowa doprowadzi do rzeczywistych, efektywnych zmian w zarządzaniu tym medium, a także jakie sfery polityki publicznej będą w tym procesie uczestniczyć i domagać się rozstrzygnięć. Pewne jest natomiast, że wszelkie potencjalne zmiany w tym zakresie mają wpływ na wolność słowa i informacji w Internecie oraz na jego umiejscowienie w systemie prawa. .

[39] Janusz Barta i Ryszard Markiewicz, Internet a prawo, op. cit.

<u>Załącznik nr 1.</u> **Objaśnienie skrótów użytych w Tabeli nr 1 i 2.**

CoE (*Council of Europe*) – Rada Europy: najstarsza organizacja polityczna w Europie (1949), skupia 46 państw, w tym 21 państw Europy Środkowej i Wschodniej, a także 5 państw-obserwatorów (Japonia, Kanada, Meksyk, Stany Zjednoczone, Stolica Apostolska) z siedzibą w Strasburgu. Działa na rzecz umacniania demokracji, praw człowieka i przestrzegania przepisów prawa. Jest również zaangażowana w umacnianie dziedzictwa kulturowego Europy ze szczególnym uwzględnieniem dorobku poszczególnych państw.

ECOSOC (*The Economic and Social Council)* – Rada Społeczno - Gospodarcza Narodów Zjednoczonych. Koordynuje prace wybranych wyspecjalizowanych organizacji Narodów Zjednoczonych, komisji funkcjonalnych oraz regionalnych, a także rozpatruje raporty funduszy i programów; udziela zaleceń systemowi NZ oraz krajom członkowskim. Z realizacją jego zadań wiąże się wykorzystanie ponad 70% zasobów ludzkich i finansowych systemu ONZ. Działając na rzecz popierania i ochrony praw człowieka, współpracuje między innymi z UNESCO, UNICEF czy FAO.

FAO – Organizacja Narodów Zjednoczonych ds. Wyżywienia i Rolnictwa, liczy 169 państw, dąży do poprawy warunków wyżywienia i warunków życia ludności, promuje rozwój rolnictwa i międzynarodowej wymiany produktów rolnych oraz poprawę warunków życia ludności wiejskiej - zapobieganie klęsce głodu.

GBDe (*Global Business Dialogue on electronic commerce*) – Globalny Dialog Biznesowy w sprawie handlu elektronicznego. Został powołany w 1999 r., jako forum dla szefów 55 światowych firm starających się promować wspólne standardy i samostanowiącą się politykę internetową.

ICANN (*The Internet Corporation for Assigned Names and Numbers*) – Internetowa Korporacja ds. Przydzielonych Nazw i Numerów: instytucja obecnie odpowiedzialna za przyznawanie nazw domen internetowych, ustalanie ich struktury oraz za ogólny nadzór nad działaniem serwerów DNS na całym świecie. Formalnie jest to prywatna organizacją non-profit, o statusie firmy zarejestrowanej w stanie Kalifornia której rząd USA przekazał czasowo prawo nadzoru nad systemem DNS i przydziałem puli adresów IPv4 oraz IPv6 dla tzw. *Regional Internet Registers* (RIR) oraz rejestrację numerów portów.

ICAO *(International Civil Aviation Organization)* – Międzynarodowa Organizacja Lotnictwa Cywilnego. Zajmuje się rozwojem techniki i organizacji międzynarodowego transportu lotniczego.

IEFT (*Internet Engineering Task Force*) – nieformalne, międzynarodowe stowarzyszenie osób zainteresowanych ustanawianiem standardów technicznych i organizacyjnych w Internecie. Nie posiada żadnej formalnej władzy, ale jej prace mają decydujący wpływ na kształt przyszłości Internetu. Generuje specjalny rodzaj dokumentów zwanych RFC, w których w formie pytań i odpowiedzi zawarta jest cała "mądrość" Internetu - wszelkie standardy techniczne i organizacyjne tworzące tę sieć.

ILO *(International Labour Organization*) – Międzynarodowa Organizacja Pracy z siedzibą w Genewie. Działa na rzecz poprawy warunków pracy, walki z bezrobociem, zagwarantowania odpowiednich zarobków, ochrony pracowników przed zagrożeniami i chorobami zawodowymi oraz ochrony pracy dzieci, młodzieży i kobiet.

ITU (*International Telecommunication Union*) – Międzynarodowy Związek Telekomunikacyjny, organizacja międzynarodowa i jedna z wyspecjalizowanych organizacji Organizacji Narodów Zjednoczonych, ustanowiona w celu standaryzowania oraz regulowania rynku telekomunikacyjnego i radiokomunikacyjnego. Głównymi zadaniami organizacji są standaryzacja i zarządzanie pasmem radiowym.

OECD (*Organisation for Economic Co-operation and Development*) – Organizacja Współpracy Gospodarczej i Rozwoju: skupia 30 wysoko rozwiniętych i demokratycznych państw, jej celem jest wspieranie państw członkowskich w osiągnięciu jak najwyższego poziomu wzrostu gospodarczego i stopy życiowej obywateli. Zajmuje się też pomocą dla najbiedniejszych państw.

ONZ (*United Nations)* – Organizacja Narodów Zjednoczonych, jej celem jest cel zapewnienie pokoju i bezpieczeństwa międzynarodowego, rozwój współpracy między narodami oraz popieranie przestrzegania praw człowieka. Jej zadania to: utrzymanie międzynarodowego pokoju i bezpieczeństwa za pomocą zbiorowych i pokojowych wysiłków, rozwijanie przyjaznych stosunków między narodami na zasadach samostanowienia i

równouprawnienia, rozwiązywanie konkretnych problemów międzynarodowych (gospodarczych, społecznych, kulturalnych, humanitarnych, czy dotyczących praw człowieka) na zasadzie współpracy międzynarodowej oraz uznania równości ras, płci, języków i wyznań, a także stanowienie ośrodka uzgadniania działań narodów w imię wspólnych celów.

UNCITRAL – Komisja ONZ do spraw Międzynarodowego Prawa Handlowego.

UNCTAD – Międzynarodowa Agencja ds. Rynku i Rozwoju: agenda ONZ obserwująca i analizująca handel międzynarodowy i zagraniczne inwestycje w świecie. Ogłaszane przez nią cyklicznie raporty są zawsze skrupulatnie analizowane i omawiane przez rządy i wszystkie liczące się ośrodki zajmujące się problematyką gospodarczą.
UNDP (*United Nations Development Programme*) – Program Narodów Zjednoczonych ds. Rozwoju. Do jego zadań należy udzielanie pomocy technicznej i finansowej krajom rozwijającym się przy opracowywaniu programów rozwoju. Współpracuje ze 166 państwami i 35 agencjami międzynarodowymi na rzecz przyspieszenia rozwoju gospodarczego. Co roku publikuje raport o rozwoju społecznym, zawierający m.in. Wskaźnik Rozwoju Społecznego (HDI - *Human Development Index)* - ranking 177 państw świata.

UNESCO (*United Nations Educational, Scientific and Cultural Organization*) – Organizacja Narodów Zjednoczonych do Spraw Oświaty, Nauki i Kultury (182 państwa członkowskie, bez USA i Wielkiej Brytanii). Jej celem jest popieranie współpracy międzynarodowej w dziedzinie kultury, sztuki i nauki, a także wzbudzanie szacunku dla praw człowieka, bez względu na kolor skóry, status społeczny i religię.

UNIDO – Organizacja Narodów Zjednoczonych ds. Rozwoju Przemysłowego z siedzibą w Wiedniu. Wyspecjalizowana organizacja działająca w ramach systemu ONZ, wspiera procesy industrializacji i pomaga krajom rozwijającym się oraz krajom znajdującym się w okresie transformacji gospodarczej w uzyskaniu należnego miejsca w coraz bardziej zglobalizowanej gospodarce światowej. Współpracując z instytucjami rządowymi i środowiskami gospodarczymi 169 państw członkowskich, promuje konkurencyjną gospodarkę, tworzenie nowych miejsc pracy i zdrowe środowisko naturalne poprzez ułatwianie dostępu do nowoczesnych technologii, pomocy technicznej i wiedzy z zakresu produkcji, zarządzania i marketingu.

UNEP (*United Nations Environmental Programme*) – Program Narodów Zjednoczonych ds. Ochrony Środowiska, z siedzibą w Nairobi; wyspecjalizowana organizacja ONZ powołana w celu koordynowania działań narodów Zjednoczonych w zakresie ochrony środowiska i stałego monitorowania stanu środowiska na świecie.

UN-Habitat *(United Nations Human Settlements Programme)* – Agenda Narodów Zjednoczonych ds. Siedzib Ludzkich. Od 2002 r. koordynuje i bezpośrednio realizuje programy pomocowe skierowane do krajów rozwijających się, dotkniętych klęskami żywiołowymi i kataklizmami.

UPU (*Universal Postal Union)* – Powszechny Związek Pocztowy. Wyspecjalizowana organizacja ONZ z siedzibą w Bernie. Główne zadania to promowanie współpracy międzynarodowej w zakresie usług pocztowych, dbanie o rozwój usług pocztowych oraz pomoc techniczna dla państw, które są jej członkami. UPU ustala również standardy przesyłek pocztowych.

W3C (World *Wide Web Consortium*) – organizacja zajmująca się ustanawianiem standardów pisania i przesyłu stron WWW. Obecnie zrzeszesza ponad 360 organizacji, firm, agencji rządowych i uczelni z całego świata; jej rekomendacje nie mają mocy prawnej, lecz wpływowość samej organizacji nie pozwala się z nimi nie liczyć.

WHO (*World Health Organization)* – Światowa Organizacja Zdrowia, organizacja działająca w ramach ONZ z siedzibą w Genewie. Działa na rzecz zwiększenia współpracy między państwami w dziedzinie ochrony zdrowia i zwalczania epidemii chorób zakaźnych, a także ustalania norm dotyczących składu lekarstw i jakości żywności. Dąży również do zapewnienia opieki medycznej ludności świata oraz zmniejszenia śmiertelności niemowląt.
WIPO (*World Intellectual Property Organisation*) – Światowa Organizacja Własności Intelektualnej: międzynarodowa instytucja zajmująca się koordynacją, tworzeniem i promocją regulacji tworzących system ochrony własności intelektualnej na świecie.

WMO *(The World Meteorological Organization*) – Światowa Organizacja Meteorologiczna; międzyrządowa organizacja skupiająca 187 członków; wyspecjalizowana organizacja ONZ,

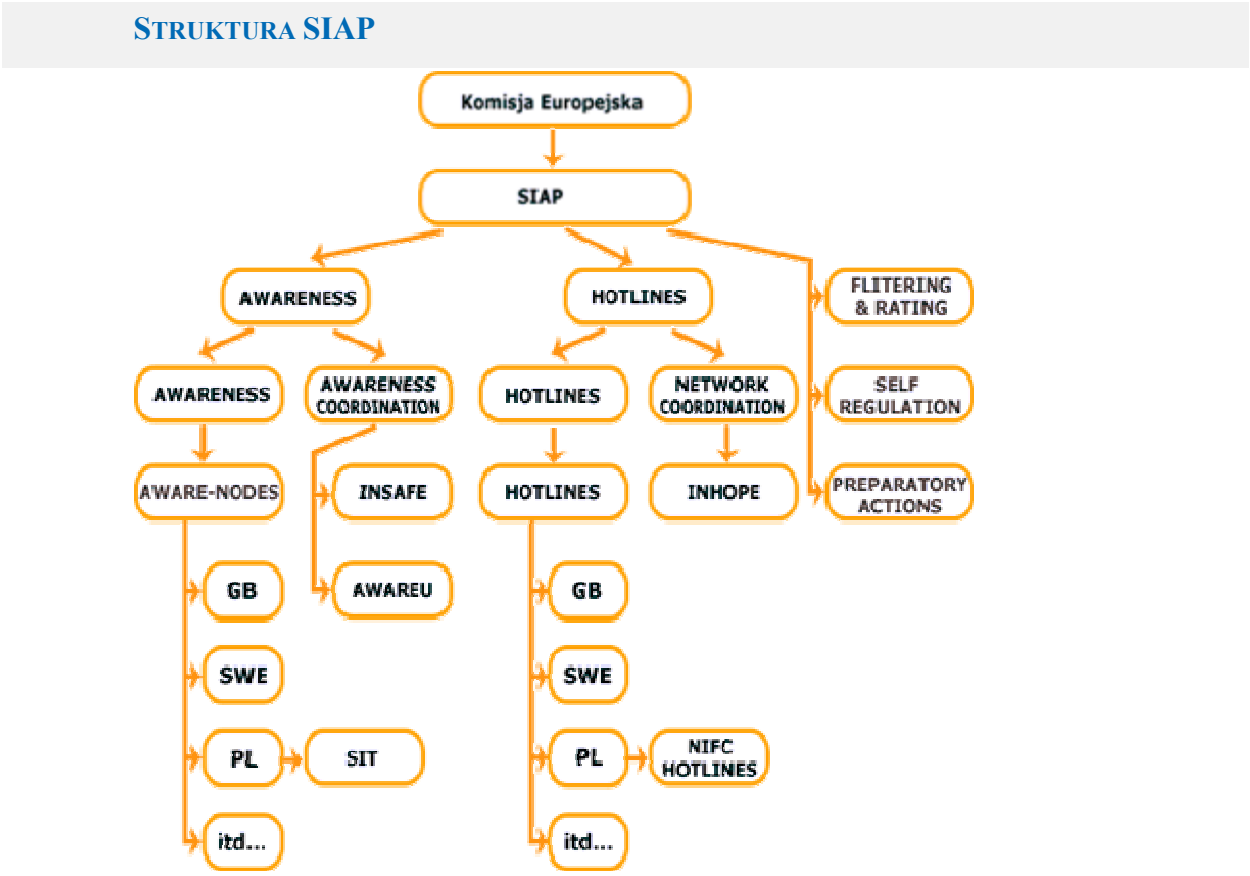
której zadaniem jest ujednolicanie, udoskanalanie i wymiana prac meteorologicznych oraz popieranie studiów klimatycznych, geograficznych i hydrologicznych.

WTO (*World Trade Organization*) – Światowa Organizacja Handlu: określa zasady współczesnego światowego handlu; posiada osobowość prawną.

Załącznik nr 2. Struktura Programu Safer Internet Action Plan, jego cele i sposoby realizacji

Wykres nr 1 przedstawia strukturę Programu Safer Internet Action Plan

Wykres nr 1. Struktura Safer Internet Action Plan (SIAP)



Źródło: http://www.dzieckowsieci.pl/media/struktura_siap.html

Ustanowienie tego programu obejmowało 4 główne cele:

- stworzenie europejskiej sieci punktów kontaktowych dla raportowania szkodliwej oraz nielegalnej treści w Internecie (*Hotlines*);
- wspieranie samoregulacji (*Self Regulation*);
- rozwój przez przemysł internetowy systemu filtrującego oraz oceniającego zawartość stron internetowy (*Filtering & Rating*);
- podniesienie świadomości o bezpiecznym użytkowaniu Internetu (*Awareness).*

Powyższe cele znalazły odzwierciedlenie w następującym Planie Działania:

1) tworzenie bezpiecznego otoczenia przez samoregulację dostawców treści;
2) rozwój systemów filtrowania i ratingu (oceniania);
3) popieranie działań uświadamiających;
4) działania wspierające.

W wyniku podjętych w Programie działań, w krajach członkowskich powstała:

- sieć 25 krajowych linii interwencyjnych „*Hotlines*”[40],
- węzeł koordynacyjny INHOPE (*Internet Hotline Providers in Europe Association*) [41], otwarty dla linii interwencyjnych z całego świata (poza Europą, „*Hotlines*” działają także w Kanadzie, USA, Korei Południowej, Australii, Nowej Zelandii i na Tajwanie);
- sieć 19 krajowych punktów podnoszenia świadomości (*Awareness*) oraz 2 punkty koordynujące funkcjonujące pod nazwą INSAFE oraz AWAREU [42].

Linie interwencyjne „*Hotlines*” działają 24 godziny na dobę, są anonimowe i nie podają policji żadnych danych osób zgłaszających. Przyjmują zgłoszenia w różny sposób (mail, telefon, faks, strona www, tradycyjna poczta), przy czym nie ma możliwości wykasowania z bazy danych raz przyjętego zgłoszenia. Po przyjęciu zgłoszenia pracownicy linii namierzają serwer, na którym umieszczone były zgłoszone nielegalne treści („*Hotlines”* okazują się praktycznie nieskuteczne w przypadku treści potencjalnie szkodliwych), następnie

[40] Wykaz *European network of hotlines* patrz: http://www.europa.eu.int/information_society/activities/sip/projects/hotlines/index_en.htm;
[41] Więcej informacji na temat INHOPE i INHOPE II: http://www.inhope.org/en/index.html oraz http://www.europa.eu.int/information_society/activities/sip/projects/hotlines/inhope_2/index_en.htm ; na temat kodeksów dobrej praktyki wdrożonych przez INHOPE: http://www.inhope.org/doc/inhope_cop.pdf
[42] Więcej informacji na temat Awareness: http://www.europa.eu.int/information_society/activities/sip/projects/awareness/index_en.htm

kontaktują się z dostawcą (*Internet Service Provider*), przy pomocy którego treści te usuwa się z serwera. W przypadku serwerów zagranicą zgłoszenie kierowane jest do odpowiedniej linii interwencyjnej w danym kraju. Dzięki współpracy z policją możliwe jest pociągnięcie do odpowiedzialności osób, które wprowadziły do sieci dane materiały, a w przypadku serwerów zagranicznych współpraca ta odbywa się za pośrednictwem Interpolu.

Jeśli chodzi o punkty podnoszenia świadomości , wchodzące w skład sieci INSAFE, to oprócz 19 punktów krajowych, z siecią tą współpracuje 6 krajów stowarzyszonych (Australia, Bułgaria, Czechy, Kanada, Rosja i Singapur) na których terytorium znajdują się organizacje dbające o bezpieczeństwo dzieci i młodzieży w Internecie.

Krajowe punkty „*Awareness"* w ramach sieci INSAFE podejmują ścisłą współpracę w celu usprawnienia procedury dzielenia się najlepszymi praktykami, informacjami oraz innymi materiałami merytorycznymi. Współpraca ta ma umożliwić podnoszenie wiedzy obywateli o bezpieczeństwie w Internecie. Członkowie sieci INSAFE monitorują oraz wychwytują wyłaniające się nowe trendy związane z użytkowaniem globalnej sieci, jednocześnie starając się podtrzymywać wizerunek Internetu jako miejsca pozyskiwania wiedzy oraz zabawy. Swoim edukacyjnym działaniem uzupełniają one działanie linii interwencyjnych *"Hotlines"*[43], prowadzą szkolenia, kampanie społeczne i informacyjne, organizują konferencje, których celem jest promowanie bezpiecznych treści oraz zmniejszenie skali zagrożeń, których źródłem może być Internet. Uczestnictwo w projekcie *"Awareness"* wymaga ponadto utrzymywania kontaktów z innymi instytucjami podejmującymi działania związane z bezpiecznym korzystaniem z Internetu. Sieć INSAFE nawołuje także do sprawiedliwego dzielenia odpowiedzialności za ochronę praw oraz potrzeb dzieci i młodzieży jako najbardziej zagrożonych w Internecie, pomiędzy rządy państw, nauczycieli, media, rodziców oraz sektor gospodarki powiązany z Internetem. Tym samym, wpisuje się ona w nurt debaty na temat odpowiedzialności za treści sprzeczne z prawem i potencjalnie szkodliwe. Wątek ten można rozwinąć i uszczegółowić poprzez podniesienie kwestii zakresu odpowiedzialności, jaką ponoszą / powinni ponosić dostawcy treści i usług oraz dostawcy dostępu do Internetu. Kwestia odpowiedzialności wywołuje w toczącej się debacie bardzo żywą polemikę, a jej złożoność dodatkowo komplikuje sprawę.

[43] Przykłady działań z Polski patrz: www.sieciaki.pl, www.dzieckowsieci.pl, www.strefawiedzy.polska.pl

<u>Załącznik nr 3:</u> **Informacja o Programie Safer Internet Plus**

Program Safer Internet Plus przewiduje następujące działania:

1) Zwalczanie treści sprzecznych z prawem;
2) Próbę zmierzenia się z treściami niechcianymi i szkodliwymi;
3) Promowanie bezpieczniejszego otoczenia;
4) Podnoszenie poziomu świadomości.

Działanie 1 pod nazwą „Zwalczanie treści sprzecznych z prawem" (25-30% budżetu Programu) przewiduje:

Obowiązkowe funkcjonowanie w krajach członkowskich i kandydujących cywilnych numerów interwencyjnych („*Hotlines")* [44].

Rolą „Hotlines" jest:

- przyjmowanie od użytkowników zgłoszeń o treściach sprzecznych z prawem, w tym także wykraczających poza pornografię dziecięcą, w celu przekazywania ich odpowiednim instancjom, do których Program zalicza dostawców usług internetowych, policję lub inny odpowiedni numer interwencyjny powołany do podejmowania dalszych kroków w tej sprawie;
- pełnienie funkcji centrów eksperckich przeznaczonych dla dostawców usług internetowych w celu udzielania im wskazówek na temat rozpoznawania treści sprzecznych z prawem;
- obowiązek przynależności do europejskiej sieci numerów interwencyjnych oraz aktywnego uczestnictwa we współpracy w ramach sieci i działań transgranicznych;
- podejmowanie i utrzymywanie kontaktów między europejską siecią „*Hotlines*" a numerami interwencyjnymi państw trzecich, szczególnie z pozostałych krajów europejskich, w których wytwarza się i umieszcza na serwerach treści sprzeczne z prawem;
- wykorzystanie funduszy europejskich do podnoszenia świadomości społecznej dotyczącej istnienia numerów interwencyjnych;

[44] Współfinansowanie z Programu nie będzie udzielane numerom interwencyjnym policji, tylko numerom cywilnym stanowiącym uzupełnienie tych pierwszych.

- w razie konieczności wsparcie finansowe dla telefonów zaufania dla dzieci, które w ten sposób mogłyby zgłaszać internetowe treści szkodliwe lub sprzeczne z prawem;
- wyznaczenie jednostki koordynującej dla każdej z sieci, w celu ułatwienia porozumienia w sprawie opracowywania na poziomie europejskim wskazówek, metod pracy i praktyk uwzględniających ograniczenia nałożone przez prawa krajowe właściwe dla poszczególnych numerów interwencyjnych.

Przewidywana rola jednostek koordynacyjących to między innymi:

- promowanie sieci jako całości, przyczynianie się w ten sposób do jej uwidocznienia na poziomie europejskim poprzez zapewnienie jednolitej tożsamości;
- kontakt z właściwymi organami w celu uzupełnienia zasięgu sieci w państwach członkowskich i krajach kandydujących;
- usprawnianie skuteczności działania sieci;
- opracowywanie wskazówek dotyczących najlepszych praktyk dla numerów interwencyjnych i dostosowywanie ich do nowych technologii;
- organizowanie regularnej wymiany informacji i doświadczeń pomiędzy numerami interwencyjnymi;
- doradztwo zespołu ekspertów i szkolenia dla nowopowstałych numerów interwencyjnych, szczególnie w krajach kandydujących;
- komunikacja z numerami interwencyjnymi w państwach trzecich;
- udział w Forum „Bezpieczniejszy Internet" i innych odpowiednich formach wymiany, w tym koordynacja wkładu/informacji zwrotnych od numerów interwencyjnych;
- monitoring skuteczności działania numerów interwencyjnych oraz zbieranie na ich temat danych statystycznych (liczba i rodzaj otrzymanych zgłoszeń, podjęte działania, osiągane wyniki, itd.). Dane te powinny być porównywalne pomiędzy państwami członkowskimi.

Działanie 2 – próba zmierzenia się z treściami niechcianymi i szkodliwymi (10-17 % budżetu Programu)

Poza działaniem mającym na celu zwalczanie treści sprzecznych z prawem u ich źródła, użytkownicy mogą potrzebować także technicznych narzędzi w celu umożliwienia im samodzielnego podejmowania decyzji w sprawie treści niepożądanych czy szkodliwych.

Jednym z celów Programu jest zatem promowanie dostępności tego typu narzędzi, finansowanie technologii umożliwiajacych ograniczanie ilości szkodliwych i niechcianych treści otrzymywanych przez użytkowników oraz sprawdzanie skuteczności dostępnych filtrów. Działanie to będzie finansować udoskonalanie filtrów oraz promować wymianę informacji i dobrych praktyk w zakresie stosowania przepisów antyspamowych (Komisja promuje w ten sposób skuteczniejszą realizację przepisów jako środek komplementarny w stosunku do istniejącego już zakazu w tym zakresie, wprowadzonego dyrektywą o ochronie życia prywatnego w sektorze komunikacji elektronicznej).

W ramach wyżej wymienionego działania przewiduje się w szczególności:

- Zapewnienie dalszego finansowania w celu pomnożenia dostępnych informacji na temat sposobu działania i skuteczności oprogramowania filtrującego i usług umożliwiających użytkownikom dokonanie świadomego wyboru.;
- Działanie systemów klasyfikacji i znaków jakości w połączeniu z technologiami filtrującymi, w celu umożliwienia użytkownikom dokonywania wyboru treści, które chcieliby otrzymywać oraz udostępnienia rodzicom i nauczycielom informacji niezbędnych do podejmowania decyzji zgodnie z ich wartościami kulturowymi i potrzebami językowymi;
- Wsparcie finansowe dla projektów mających na celu dostosowanie systemów klasyfikacji i znaków jakości, tak aby uwzględniały one konwergencję telekomunikacji, mediów audiowizualnych i technologii informacyjnej oraz wsparcie dla inicjatyw w zakresie samoregulacji mających na celu wzmocnienie wiarygodności znakowania oraz usług oceniających zasadność samo-klasyfikacji;
- Położenie nacisku na uwzględnianie bezpieczeństwa małoletnich użytkowników na etapie opracowywania nowych technologii zamiast ograniczania się do naprawiania szkód wynikających z niedostatecznie bezpiecznego ich wykorzystywania. Decyzja ustanawiająca Program uzasadnia to stwierdzeniem, że bezpieczeństwo końcowego użytkownika stanowi równoprawne kryterium w stosunku do kryteriów technicznych i rynkowych oraz zachęca do współpracy ekspertów technicznych i specjalistów w zakresie ochrony dzieci, a także deklaruje wsparcie finansowe na rzecz środków technologicznych umożliwiających użytkownikom ograniczenie ilości niechcianych i szkodliwych treści oraz zarządzanie otrzymywanym spamem.

Finansowanie w tym działaniu obejmie między innymi:

- ocenę skuteczności dostępnych technologii filtrujących oraz informowanie na ten temat opinii publicznej w zrozumiałej i prostej formie ułatwiającej dokonanie porównania dostępnych technologii w tym zakresie;
- środki ułatwiające i koordynujące wymianę informacji i najlepszych praktyk w zakresie sposobów skutecznego radzenia sobie z niechcianymi i szkodliwymi treściami;
- poprawę w korzystaniu przez dostawców treści z systemów klasyfikacji treści oraz znaków jakości witryn internetowych, a także dostosowanie tych ostatnich do tego, by można było korzystać z tych samych treści za pomocą różnych platform dostępu (uwzględnienie efektów konwergencji);
- jeżeli to konieczne, przyczynianie się do dostępności technologii filtrujących w wersjach językowych niewystarczająco pokrywanych przez rynek.

Działanie 3: Promowanie bezpieczniejszego otoczenia (działania samoregulacyjne) na które przeznacza się 8-12 % budżetu Programu

Punktem wyjścia dla tego Działania jest przekonanie Parlamentu i Rady Unii Europejskiej, że dobrze funkcjonujący system samoregulacji stanowi zasadniczy element ograniczenia przepływu niechcianych, szkodliwych i sprzecznych z prawem treści, natomiast nowym elementem jest przeznaczenie wsparcia finansowego dla projektów mających na celu opracowanie transgranicznych, a nie tylko krajowych kodeksów postępowania.

W wydaniu Programu Safer Internet Plus samoregulację tworzą następujące elementy:

- konsultacja i odpowiednia reprezentacja zainteresowanych stron;
- kodeksy postępowania (Program dostrzega konieczność kontynuowania działań na poziomie wspólnotowym na rzecz zachęcania europejskiego przemysłu internetowego i nowych technologii sieciowych do wdrażania kodeksów postępowania);
- odpowiednie instytucje krajowe ułatwiające współpracę na poziomie wspólnotowym;
- ewaluacja samoregulacji realizowana na poziomie krajowym [45] .

[45] Patrz. kierunki samoregulacji na poziomie krajowym w zakresie ochrony nieletnich i godności ludzkiej zawarte w Zaleceniu 98/560/WE .

Inną inicjatywą wpisującą się w ramy tego Działania jest działające od 2004 r. Forum „Bezpieczniejszy Internet". Stanowi ono ważne miejsce spotkań i forum dyskusyjne dla wszystkich zainteresowanych stron pochodzących również spoza krajów członkowskich i kandydujących - przedstawicieli przemysłu, organów państwowych odpowiedzialnych za wdrażanie prawa, polityków, agencji i programów rządowych, organów normalizacyjnych, przemysłu, służb Komisji Europejskiej oraz organizacji użytkowników, do których Program zalicza między innymi organizacje rodziców i nauczycieli, grupy zajmujące się ochroną dzieci, organizacje konsumenckie i obywatelskie. Forum jest również platformą wymiany doświadczeń pomiędzy krajowymi organami w zakresie współregulacji oraz podmiotami samoregulującymi się w zakresie sposobów zwalczania przez te nie treści sprzecznych z prawem. Forum pełni rolę platformy w poszukiwaniu konsensusu i wypracowywaniu wspólnych wniosków, zaleceń i kierunkowych propozycji dla zaangażowanych stron na poziomie krajowym i wspólnotowym. Łączy i stymuluje działania oraz ułatwia debatę.

Działanie 4: Podnoszenie poziomu świadomości (47-51% budżetu Programu)

Inicjatywy i projekty podejmowane w ramach tego Działania dotyczą obszaru, który wykracza poza przedmiot zainteresowania niniejszego opracowania, czyli zawartość Internetu (*content*). Obejmują one nie tylko treści sprzeczne z prawem i treści szkodliwe, ale także treści niechciane, a tam gdzie to konieczne, zagadnienia związane z ochroną konsumentów, ochroną danych oraz bezpieczeństwem informacji i sieci (wirusy/spam), jak również nowe formy interaktywnej informacji i komunikacji, które powstały w wyniku szybkiego rozprzestrzeniania się Internetu i telefonii komórkowej (np.: usługi typu (*peer-to-peer*, szerokopasmowa transmisja wideo, komunikatory internetowe, czaty itd.).

W ramach tego Działania, zostanie udzielone wsparcie finansowe dla podmiotów pełniących rolę jednostek odpowiedzialnych za podnoszenie świadomości w poszczególnych państwach członkowskich i kandydujących. Ich zadaniem będzie prowadzenie działań i projektów uświadamiających w ścisłej współpracy ze wszystkimi stronami na poziomie krajowym, regionalnym i lokalnym, a europejską wartość dodaną zapewni utworzenie jednostki koordynującej.

Jednostki odpowiedzialne za podnoszenie poziomu świadomości będą zobowiązane do:

- opracowywania spójnej, dynamicznej i skierowanej do określonych grup odbiorców kampanii społecznej prowadzonej w odpowiednich do tego celu mediach z uwzględnieniem najlepszych praktyk i doświadczeń innych krajów w tym zakresie;
- budowy i podtrzymywania formalnych i nieformalnych stosunków partnerskich z głównymi zainteresowanymi stronami (agencjami rządowymi i pozarządowymi, mediami, dystrybutorami usług oraz użytkownikami Internetu) oraz do działania na poziomie kraju na rzecz bezpieczniejszego korzystania z Internetu i nowych technologii sieciowych;
- promowania dialogu i wymiany informacji, szczególnie pomiędzy zainteresowanymi stronami w dziedzinie edukacji i technologii;
- informowania użytkowników o europejskim oprogramowaniu i usługach filtrujących, jak również o numerach interwencyjnych i systemach samoregulacji;
- aktywnej współpracy w ramach sieci, w tym do wymiany informacji na temat najlepszych praktyk oraz opracowywania i realizacji europejskiego podejścia, dostosowanego do krajowych preferencji językowych i kulturowych;
- zapewnienia wiedzy eksperckiej i technicznego wsparcia dla nowopowstających jednostek.

Załącznik nr 4. **Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)16 w sprawie ochrony dzieci przed seksualnym wykorzystywaniem (2001);**

oraz

Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)8 dotycząca samoregulacji w zakresie cyber-zawartości: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych (2001).

Rekomendacja Komitetu Ministrów Rec(2001)16 w sprawie ochrony dzieci przed seksualnym wykorzystywaniem (2001)

Zaleca ona między innymi:

- Włączenie dostawców usług internetowych w prace nad podnoszeniem świadomości na temat seksualnego wykorzystywania dzieci i związanych z tym zagrożeń, zwłaszcza za pomocą Internetu i z zastosowaniem nowoczesnych technologii telekomunikacyjnych;
- Zagwarantowanie, by dostawcy usług internetowych działali we współpracy z władzami w celu identyfikowania i zwalczania różnych sposobów zastosowania Internetu do seksualnego wykorzystywania dzieci;
- Zachęcanie dostawców usług internetowych do stworzenia kodeksu postępowania dostosowanego do nowoczesnych technologii informacyjnych i telekomunikacyjnych w celu zapobiegania seksualnemu wykorzystywaniu dzieci, a także identyfikowanie przypadków naruszania takiego kodeksu oraz podejmowanie środków zapobiegawczych i zwalczających takie praktyki ;
- Uznanie, że służby ścigania muszą mieć możliwość korzystania z danych o połączeniach w celu śledzenia podejrzanych treści, a następnie lokalizowania, identyfikowania i przesłuchiwania osób zamieszczających lub upowszechniających dziecięcą pornografię lub też zachęcających / namawiających do dziecięcej prostytucji;
- Przekazywanie rodzicom, opiekunom i innym osobom odpowiedzialnym za dzieci oraz samym dzieciom informacji o zagrożeniach związanych z seksualnym

wykorzystywaniem przez Internet, o postaciach, jakie może przyjmować takie wykorzystywanie;

- Wprowadzenie specjalnych linii telefonicznych oraz zachęcanie obywateli do informowania o przypadkach dziecięcej pornografii lub namawiania do dziecięcej prostytucji na stronach internetowych, co umożliwi odpowiednim służbom ścigania podjęcie konkretnych działań w tym zakresie.

Rekomendacja Komitetu Ministrów Rec(2001)8 dotycząca samoregulacji w zakresie cyber-zawartości: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych (2001);

Uzasadnienie towarzyszące Rekomendacji wyraźnie stwierdza, że:

- Co prawda sektor prywatny, a w szczególności przemysł nowych usług informacyjno-komunikacyjnych nie jest bezpośrednim adresatem tej Rekomendacji, niemniej jednak to do państw członkowskich należy podjęcie odpowiednich kroków w celu włączenia tego sektora do realizacji zaleceń niniejszej Rekomendacji;
- Termin „treści" należy rozumieć jako każdy rodzaj zawartości w nowych usługach komunikacyjno-informacyjnych, a więc zarówno tekst, obraz i dźwięk jak i komunikację interaktywną, jako że cechą tych usług jest łączenie powyższych elementów.

Ponadto, Uzasadnienie to daje wykładnię treści nielegalnych (treści sprzeczne z prawem krajowym) oraz szkodliwych, ujmując te ostatnie jako niekoniecznie nielegalne, za to potencjalnie niosące szkodę, szczególnie dla fizycznego, psychicznego i moralnego rozwoju nieletnich.

Zgodnie z powyższą Rekomendacją rolą państw członkowskich w zakresie promowania bezpiecznego korzystania z Internetu jest:

- Zachęcanie dostawców treści i usług internetowych do tworzenia wraz z użytkownikami reprezentujących ich organizacji;
- Zachęcanie wyżej wymienionych organizacji do tworzenia mechanizmów samoregulujących, na przykład w postaci kodeksów postępowania, w tym szczególnie do kontroli przestrzegania zawartych w nim zasad;

- Zachęcanie organizacji medialnych do stosowania norm samoregulujących do - w miarę możliwości - nowych usług informacyjno-komunikacyjnych (w tym Internetu);
- Zachęcanie wyżej określonych organizacji do uczestnictwa w procesach legislacyjnych ich dotyczących, na przykład w postaci konsultacji, wysłuchań czy zasięgania opinii eksperckich;
- Zachęcanie wyżej określonych organizacji do wymiany i współpracy na poziomie międzynarodowym (zarówno w Europie jak i z innymi krajami);
- Zachęcanie do określania w możliwie najszerszej skali geograficznej i we współpracy z powyższymi organizacjami pełnego zestawu opisów treści (*a set* of *content descriptors*) umożliwiających neutralne znakowanie zawartości Internetu w celu umożliwienia użytkownikom wyrobienia własnego zdania na temat konkretnych treści w Internecie (opisy te powinny określać nie tylko treści pornograficzne czy związane z przemocą, ale też nawołujące do korzystania z gier pieniężnych, picia alkoholu czy palenia papierosów lub umożliwiające niekontrolowane i anonimowe kontakty nieletnich z dorosłymi);
- Zachęcanie dostawców treści do stosowania powyższych opisów w celu umożliwienia użytkownikom rozpoznawania i filtrowania treści bez względu na ich pochodzenie;
- Tworzenie szerokiej gamy narzędzi pełniących rolę wyszukiwarek i filtrów zawartości, umożliwiających użytkownikom Internetu selekcję treści na podstawie wyżej wymienionych opisów, przy czym wybór systemu filtrowania powinien być pozostawiony swobodnej decyzji użytkowników.
- Stosowanie narzędzi warunkowego dostępu w zakresie treści szkodliwych dla nieletnich, takich jak systemy weryfikacji wieku [46], osobiste kody identyfikacyjne, hasła, systemy kodowania lub dostęp za pomocą kart elektronicznych;
- Zachęcanie do tworzenia systemów zgłoszeniowych dla treści nielegalnych (zalecane struktura i opis działania takich systemów przypomina unijne „Hotlines") uzupełnionych o komplementarne, bezpośrednie linie uruchomione przez władze publiczne;
- Opracowanie z instytucjami publicznymi ram współpracy w zakresie systemów zgłaszania treści nielegalnych, w tym określenie przez państwa członkowskie zakresów odpowiedzialności i prawnych przywilejów dla instytucji prowadzących punkty

[46] System weryfikacji wieku proponuje też projekt amerykańskiej ustawy z 29.06.2005 r. *A Bill to protect children from Internet pornography and support law enforcement and other efforts to combat Internet and pornography-related crimes against children*.

zgłoszeniowe w zakresie dostępu, kopiowania i gromadzenia treści nielegalnych oraz ich przekazywania organom ścigania [47];

- Zachęcanie krajowych punktów zgłoszeniowych do wymiany i współpracy z analogicznymi punktami z innych krajów oraz spowodowanie za pomocą środków prawnych i administracyjnych transgranicznej wymiany między organami ścigania w zakresie treści nielegalnych pochodzących z zagranicy;
- Zachęcanie do tworzenia na poziomie krajowym dobrowolnych, niezależnych, dostępnych i skutecznych organów i procedur w zakresie mediacji oraz mechanizmów arbitrażu w zakresie sporów dotyczących treści w Internecie;
- Zachęcanie powyższych organów mediacyjnych i arbitrażowych do międzynarodowej współpracy, w tym do wzajemnego uznawania swoich orzeczeń, a także do swobodnego dostępu do tych procedur dla wszystkich chętnych bez względu na granice państwowe;
- Zachęcanie do tworzenia znaków jakości (*quality labels*) dla treści rozpowszechnianych w Internecie, na przykład dla treści pochodzących od organów administracji państwowej, treści o charakterze pedagogicznym lub treści przeznaczonych dla dzieci, co znacznie ułatwiałoby wyszukiwanie i identyfikację tego typu treści;
- Zachęcanie do prowadzenia działań informacyjnych i uświadamiających w zakresie mechanizmów samoregulacji, opisów zawartości, narzędzi filtrujących i narzędzi ograniczających dostęp do określonych treści, systemów zgłoszeniowych treści nielegalnych oraz procedur mediacyjnych i arbitrażowych.

SPIS TREŚCI

[47] Polski „Hotline" o nazwie „Dyżurnet" boryka się z problemem, który ogranicza skuteczność jego działania, a dotyczy właśnie braku uregulowania w zakresie gromadzenia i kopiowania treści nielegalnych.

b) Stanowisko pośrednie (Unia Europejska i Rada Europy)

c) Kraje autokratyczne: zaprzeczenie zasady swobody wypowiedzi i informacji w Internecie

3) Swoboda wypowiedzi i informacji w Internecie a walka z terroryzmem

a) Unia Europejska

b) USA

c) Rada Europy

d) ARTICLE 19

4) Dopuszczalne ograniczenia w zakresie swobody wypowiedzi i informacji w Internecie ze względu na potrzebę ich zrównoważenia z innymi prawami i swobodami obywatelskimi

a) Zapobieganie treściom nielegalnym i potencjalnie szkodliwym

b) Internet: zastosowanie prawa ogólnego

i) Unia Europejska

ii) Rada Europy

c) Regulacje prawne stworzone specjalnie dla Internetu

i) Rada Europy

ii) Unia Europejska

(1) Program Safer Interent Action Plan (SIAP)

(2) Ewolucja w postawie Unii Europejskiej

(3) Program Safer Internet Plus

iii) USA

iv) Hiszpania i Niemcy

v) Australia i Francja

d) „Miękkie prawo" (wyznacza kierunki działania, lecz nie posiada mocy prawnej) odnoszące się do Internetu

i) Unia Europejska

ii) Rada Europy

e) Samoregulacja
   i) Organizacje samoregulacyjne
   ii) Internet Watch Fundation
   iii) Kodeksy dobrej praktyki / kodeksy postępowania

5) Problemy jurysdykcyjne i trudności z przypisaniem odpowiedzialności w zakresie nadużyć swobody wypowiedzi i informacji w Internecie

a) Odpowiedzialność dostawców usług internetowych
b) Odpowiedzialność poszczególnych państw
   i) Rada Europy
   ii) USA vs. Francja
   iii) Australia

6) Zakończenie

Załącznik nr 1. Objaśnienie skrótów użytych w Tabeli nr 1 i 2.

Załącznik nr 2. Struktura Programu Safer Internet Action Plan, jego cele i sposoby realizacji

Załącznik nr 3: Informacja o Programie Safer Internet Plus

Załącznik nr 4. Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)16 w sprawie ochrony dzieci przed seksualnym wykorzystywaniem (2001);
oraz
Rekomendacja Komitetu Ministrów Rady Europy Rec(2001)8 dotycząca samoregulacji w zakresie cyber-zawartości: samoregulacja oraz ochrona użytkowników przed treściami nielegalnymi i szkodliwymi w usługach informacyjno-komunikacyjnych (2001).