5.8 EKES jest zdania, że rozporządzenie nr 4056/86 powinno zostać uchylone i zastąpione nowym rozporządzeniem Komisji w sprawie wyłączenia grupowego dla konferencji żeglugowych. Nowy system powinien być ściśle oparty na wytycznych ustanowionych na podstawie orzecznictwa Europejskiego Sądu Pierwszej Instancji i Komisji (np. na sprawie TACA). Poza tym powinno się utrzymać system konferencji również dlatego, by chronić konkurencyjność armatorów UE w skali światowej. Podczas gdy w przypadku dużych armatorów właściwe mogłyby być sojusze i inne rodzaje porozumień o współpracy, to mali i średni przewoźnicy potrzebują nadal konferencji, by utrzymać swój udział w rynku, przede wszystkim w zakresie morskiej wymiany handlowej z krajami rozwijającymi się. Uchylenie tego wyłączenia mogłoby doprowadzić do pogorszenia konkurencyjności mniejszych armatorów i wzmocnienia dominującej pozycji dużych przedsiębiorstw.

5.9 Okres przejściowy powinien zostać wykorzystany przez Komisję do monitorowania zmian na rynku żeglugi liniowej, a także trendów konsolidacyjnych. Ponadto, Komisja powinna rozpocząć konsultacje z państwami innych systemów jurysdykcyjnych (OECD) by wypracować odpowiedni alternatywny system, pozostający w zgodzie z prawem na całym świecie.

5.10 EKES popiera zawarte w Białej Księdze propozycje dotyczące traktowania usług żeglugi trampowej i kabotażowej, gdyż w przeważającej większości przypadków w tych sektorach nie ma żadnych problemów w zakresie konkurencji. Ze względu na pewność prawną, proponuje się, aby Komisja ustanowiła wytyczne prawne służące do samooceny konsorcjów ładunków masowych i sektorów około-żeglugowych w zakresie ich zgodności z art. 81 Traktatu ustanawiającego Wspólnotę Europejską.

5.11 EKES wyraża nadzieję, że będzie mógł zaoferować swój udział w dalszych pracach zainicjowanych burzą mózgów wywołaną przez Białą Księgę.

Bruksela, dn. 16 grudnia 2004 r.

*Przewodnicząca*
*Europejskiego Komitetu Ekonomiczno-Społecznego*
Anne-Marie SIGMUND

---

## Opinia europejskiego komitetu ekonomiczno-społecznego w sprawie wniosku dotyczącego decyzji parlamentu europejskiego i rady ustanawiającej wieloletni wspólnotowy program promocji bezpieczniejszego korzystania z internetu i nowoczesnych technologii online

*COM(2004) 91 końcowy — 2004/0023 (COD)*

(2005/C 157/24)

Dnia 26 marca 2004 r. Rada, działając na podstawie art. 153 Traktatu ustanawiającego Wspólnotę Europejską, postanowiła zasięgnąć opinii Europejskiego Komitetu Ekonomiczno-Społecznego w sprawie wspomnianej powyżej

Sekcja ds. Transportu, Energii, Infrastruktury i Społeczeństwa Informacyjnego, której powierzono przygotowanie prac Komitetu w tej sprawie, sporządziła swą opinię 5 października 2004 r. Sprawozdawcą był Daniel RETUREAU (współsprawozdawca: Ann DAVISON).

Na 413. sesji plenarnej w dniach 15-16 grudnia 2004 r. (posiedzenie z dnia 16 grudnia 2004 r.) Europejski Komitet Ekonomiczno-Społeczny 147 głosami, przy jednym głosie wstrzymującym się, przyjął następującą opinię:

### 1. **Streszczenie projektu opinii**

1.1 Komisja proponuje uruchomienie nowego programu *„Safe Internet”*, wzmocnionego jednak ze względu na szybki rozwój społeczeństwa informacyjnego w dziedzinie sieci telekomunikacyjnych. Dlatego też program został nazwany *„Safe Internet plus”* (2005-2008).

1.2 Oprócz przedstawionej przez Komisję propozycji decyzji Parlamentu i Rady Komitet przeanalizował również wstępną ewaluację projektu *Safer Internet plus* (2005-2008) zawartą w „Commission Staff working paper” SEC(2004) 148 i COM(2004) 91 końcowy. Komitet popiera rozszerzenie zakresu nowego planu działania oraz jego cele, uwzględniające szybki rozwój i różnorodność sposobów dostępu do sieci oraz bardzo szybką popularyzację szybkiego dostępu do Internetu i stałych łącz. W swych uwagach ogólnych i szczegółowych Komitet przedstawia dodatkowe propozycje działań politycznych i normatywnych, w szczególności dotyczące:

— norm technicznych i prawnych (obowiązkowych i fakultatywnych);

— edukacji i szkolenia użytkowników;

— obowiązków podmiotów świadczących usługi internetowe oraz innych operatorów (firm obsługujących karty kredytowe, wyszukiwarek internetowych itp.);

— odpowiedzialności autorów oprogramowania i osób świadczących usługi w zakresie bezpieczeństwa w sieci;

— ochrony użytkowników mogących stanowić łatwy cel przed oszustwami i niewiarygodnymi informacjami (oszustwami wszelkiego rodzaju, „wolną" sprzedażą aktywnych leków, porady lub terapia oferowana przez osoby nieuprawnione itp.).

2. **Propozycje Komisji (streszczenie)**

2.1 Celem proponowanego programu jest promocja bezpiecznego korzystania z Internetu i technologii *online* przez użytkownika końcowego, w szczególności przez dzieci i młodzież, zarówno w domu, jak i w szkole. Przewiduje się w związku z tym dofinansowywanie przygotowanych przez stowarzyszenia i inne podmioty (zespoły naukowo-badawcze, projektantów oprogramowania, szkoły itp.) projektów rozwoju środków ochrony użytkowników, np. specjalistycznych infolinii, programów antyspamowych i antywirusowych czy „inteligentnych" filtrów nawigacyjnych.

2.2 Poprzedni plan na rzecz bezpiecznego Internetu (1999-2002) został przedłużony na lata 2003-2004.

2.3 Na stronie internetowej Komisji ([1]) znajduje się wykaz projektów zrealizowanych w ramach programu *Safe Internet* do końca 2003 r.

2.4 Obecny wniosek (2005-2008) obejmuje również nowe sposoby komunikacji w sieci, w odniesieniu do których Komisja zamierza nasilić zwalczanie treści nielegalnych i szkodliwych, w tym wirusów i innych treści krzywdzących lub niepożądanych (spam).

2.5 Bardziej energicznego zwalczania takich treści wymaga w oczach instytucji wspólnotowych szereg przyczyn, przede wszystkim:

— szybkie upowszechnianie się dostępu szerokopasmowego z połączeniami długotrwałymi lub stałymi łączami wśród osób fizycznych, przedsiębiorstw, w administracji i instytucjach prywatnych (organizacjach pozarządowych);

— różnorodność środków i metod dostępu do Internetu oraz do nowych umieszczanych w nim materiałów, z których wiele jest niepożądanych (maile, SMS) rosnąca atrakcyjność tych treści (multimedia);

— gwałtowne rozprzestrzenianie się treści niepożądanych i potencjalnie niebezpiecznych lub niewłaściwych stwarza nowe zagrożenia dla ogółu społeczeństwa (wirusy — zajmowanie przestrzeni na dysku, sprzeniewierzenie lub zniszczenie danych, niedozwolone użycie środków telekomunikacji poszkodowanego; niezamówione treści reklamowe (tzw. spam) — zawłaszczenie częstotliwości transmisyjnych oraz przestrzeni na dysku, przeładowanie skrzynek poczty elektronicznej, co uniemożliwia lub utrudnia skuteczne korzystanie z Internetu i telekomunikacji oraz pociąga za sobą znaczne koszty ponoszone nie przez osoby odpowiedzialne, lecz przez użytkownika końcowego) oraz dla niektórych ważnych kategorii użytkowników, jak dzieci (spam o jednoznacznie pornograficznej treści, nieprzyzwoite wiadomości oraz oferty spotkań zamieszczane przez pedofilów na tzw. czatach);

— łatwa dostępność dla dzieci treści niestosownych dla nich z powodu bardzo ograniczonej skuteczności obecnych na rynku środków filtrujących przeznaczonych dla opiekunów dzieci.

2.6 Głównym celem programu jest ochrona dzieci i wspieranie osób za nie odpowiedzialnych (rodzice, nauczyciele, wychowawcy itd.) lub broniących ich interesów moralnych i ich dobra. Jest on więc adresowany do organizacji pozarządowych działających w sektorze społecznym, w zakresie praw dziecka, zajmujących się zwalczaniem rasizmu, ksenofobii ([2]) i wszelkich postaci dyskryminacji, ochroną konsumentów, swobód obywatelskich itp.

2.7 Dotyczy on również rządów, organów ustawodawczych, wymiaru sprawiedliwości i policji oraz organów regulacyjnych. Niezbędne jest odpowiednie dostosowanie prawa materialnego i procesowego oraz przeszkolenie i wyposażenie dostatecznej liczby personelu.

2.8 Program dotyczy również przemysłu, który potrzebuje bezpiecznego otoczenia, by pozyskać większe zaufanie konsumentów.

2.9 Uczelnie oraz badania naukowe mogą wyjaśniać sposoby wykorzystywania nowoczesnych mediów przez dzieci. Najlepszą drogą przekazywania informacji na temat bezpieczeństwa jest informowanie o sposobach postępowania przestępców działających za pośrednictwem tych mediów, poszukiwanie nowych rozwiązań technicznych oraz przedstawianie niezależnego punktu widzenia w kwestii pogodzenia interesów podmiotów, których dotyczyć ma regulacja i samoregulacja.

2.10 Program ma dwa wymiary. W wymiarze społecznym skupia się na dziedzinach, w których regulacja i rynek nie są w stanie na własną rękę zapewnić użytkownikom bezpieczeństwa. W wymiarze gospodarczym chodzi o promowanie bezpiecznego korzystania z Internetu i technologii online poprzez tworzenie atmosfery wzajemnego zaufania.

2.11 Na dofinansowanie prac nad środkami technicznych i prawnych, oprogramowaniem oraz informacją przewidziano około 50 mln euro; celem jest podejmowanie skutecznej walki z atakami na sieci i na terminale oraz z ich nieuczciwym wykorzystywaniem do rozsyłania treści niepożądanych lub szkodliwych pod względem moralnym, społecznym bądź gospodarczym.

([1]) http://www.europa.eu.int/information_society/programmes/iap/index_en.htm

([2]) Taki zestaw zagadnień odpowiada formułowanym wcześniej przez Komitet sugestiom.

3. **Uwagi ogólne Komitetu**

3.1 Komitet przypomina swoje poprzednie opinie w sprawie ochrony dzieci w Internecie i pierwszej edycji planu działania ([1]). Pozytywnie ocenia propozycję nowego planu walki z treściami nielegalnymi lub szkodliwymi w komunikacji w sieci (patrz punkt 1. — Streszczenie). Popiera cele i priorytety programu *Safer Internet plus* jako jednego z mechanizmów służących poprawie bezpieczeństwa w Internecie. Komitet podkreśla jednak, że jest to ogromny problem i że stawienie mu czoła wymaga działań i uregulowań międzynarodowych.

3.2 Sieć internetowa i nowe technologie komunikacji w sieci (na przykład dynamicznie upowszechniające się telefony komórkowe i urządzenia typu palmtop zawierające funkcje multimedialne) są w oczach Komitetu podstawowymi instrumentami rozwoju gospodarki opartej na wiedzy oraz gospodarki i administracji elektronicznej. Stanowią one również wszechstronne narzędzia służące komunikowaniu się, korzystaniu z kultury, pracy i spędzaniu czasu wolnego. Najważniejsze jest zatem zapewnienie bezpieczeństwa i ciągłości funkcjonowania sieci komunikacyjnych, ponieważ chodzi o istotne usługi dla społeczeństwa, które powinny być otwarte, dostępne i do których wszyscy użytkownicy powinni mieć zaufanie, aby móc korzystać z ich licznych funkcji w jak najlepszych warunkach. Jednym z najbardziej obiecujących pod względem efektywności ekonomicznej sposobów docierania do znaczącej liczby osób jest włączenie informacji o bezpieczeństwie Internetu do różnych programów e-Europa, w szczególności w dziedzinie kształcenia.

3.3 Panującej w Internecie swobodzie wypowiedzi i komunikacji sprzyja stosunkowo niski koszt połączeń, w tym także szerokopasmowych, które umożliwiają coraz łatwiejszy dostęp do treści multimedialnych. Kontrolować dostęp do internetu i jego zawartość usiłują jedynie nieliczne kraje o wysokim deficycie demokracji; odbywa się to za cenę nieustannego naruszania wolności ich obywateli. Komitet uważa, iż należy zapewnić większe bezpieczeństwo, zachowując jednocześnie i popierając swobodę przepływu informacji, komunikowania się i wypowiedzi.

3.4 Jednakże, przestrzeń swobody słowa i przepływu informacji, którą jest sieć globalna, jest również wykorzystywana, w stopniu większym niż inne środki przekazu, do nielegalnych działań jak na przykład pedofilia lub rozpowszechnianie treści rasistowskich i ksenofobicznych; pewne treści mogą również okazać się szkodliwe dla niektórych osób, w szczególności dla nieletnich, jak na przykład pornografia lub gry hazardowe (nielegalne w niektórych państwach) i różne działania przestępcze (zawłaszczenie częstotliwości transmisyjnych lub wykorzystanie danych i serwerów do celów niezgodnych z prawem). Komitet popiera rozszerzenie planu działania na całość elektronicznych środków łączności, które mogą być przedmiotem niepożądanego lub wrogiego dostępu z zewnątrz.

3.5 Regulowanie tej nowej, przezywającej dynamiczny rozwój przestrzeni jest niełatwe ze względu na to, iż jest ona siecią międzynarodową, powszechnie otwartą i dostępną z każdego serwera i terminala łączącego się bez ograniczeń z niemal każdego państwa świata. W wielu państwach jednak zawodne lub niewystarczające ustawodawstwo umożliwia kontynuowanie działalności stronom internetowym zakazanym w Europie. Istotne jest, by Unia Europejska opowiedziała się na rzecz międzynarodowego wysiłku i podjęła w tym kierunku odpowiednie działania — w szczególności wspólnie z najważniejszymi krajami, w których rozpowszechniony jest szerokopasmowy dostęp do Internetu w Ameryce Północnej i Azji — w celu zapewnienia ochrony użytkownikom stanowiącym najłatwiejszy cel oraz skuteczniejszej walki z niezamówionymi reklamami (tzw. spamem), które zagrażają rozwojowi poczty elektronicznej, oraz z rozprzestrzenianiem się wirusów, które szkodzą gospodarce opartej na technologii cyfrowej. Chociaż środki, które należy wdrożyć, niezbędne są w europejskiej przestrzeni wspólnotowej, powinny również wpisywać się w kontekst ogólnoświatowy.

3.6 Ponieważ brak w tej dziedzinie porozumień międzynarodowych, zakazanie niektórych treści w niektórych krajach może być nawet przedmiotem skargi w WTO na gruncie TBT ([2]); kwestia ta powinna stanowić przedmiot bieżącej rundy negocjacji.

3.7 Terytorialny charakter prawa i różnorodność ustawodawstw krajowych stanowi trudną do pokonania barierę. Stan technologii pozwala również na wymianę dowolnych plików bezpośrednio między dowolnymi osobami (P2P — peer to peer), w tym plików zaszyfrowanych, których treści nie sposób poddać kontroli. Dowolny komputer lub sieć z dostępem do Internetu można wykorzystywać do przechowywania lub przesyłania coraz bardziej złożonych treści. Technologia umożliwia również anonimowe i niewykrywalne łączenie się z dowolnym serwerem oraz używanie bardzo złożonych lub wręcz „niemożliwych do złamania" sposobów szyfrowania.

3.8 Moda na osobiste strony internetowe i na tzw. blogi (pamiętniki internetowe), rozwój stron komercyjnych czy elektronicznych usług finansowych, różnorodność stron informacyjnych, edukacyjnych, naukowych lub technicznych, ale również pornograficznych lub stron związanych z grami hazardowymi itd. doprowadziła do powstania setek milionów stron na całym świecie. Możliwe jest jednak prowadzenie pewnej kontroli przy sporządzaniu indeksów słów kluczowych dla wyszukiwarek. Bezpośrednie połączenia i strony przeznaczone do automatycznego rozsyłania swojej zawartości, np. spamu, również mogą podlegać kontroli ze strony dostawców dostępu do Internetu: reklamy i inne treści niepożądane wysyłane w ten sposób mogą mieć charakter szkodliwy dla ogółu (zawłaszczenie częstotliwości, wirus) lub dla niektórych adresatów, np. dzieci (szkody moralne lub psychologiczne).

([1]) Opinie EKES w sprawie programu ochrony dzieci w Internecie, sprawozdawca – Ann DAVISON, Dz.U. C 48 z 21/02/2002 oraz w sprawie komunikatu Komisji do Rady; Parlamentu Europejskiego, Europejskiego Komitetu Ekonomiczno-Społecznego „Bezpieczeństwo sieci i informacji – propozycja w sprawie europejskiego podejścia politycznego", sprawozdawca – Daniel RETUREAU, Dz.U. C 48 z 21/02/2002, jak również w sprawie zielonej księgi w sprawie ochrony nieletnich i godności ludzkiej w usługach audiowizualnych i informacyjnych, sprawozdawca – Jocelyn BARROW, Dz.U. C 287 z 22/09/1997.

([2]) „Technical Barriers to Trade" – umowy w sprawie technicznych barier dla handlu i usług. Por. np. sprawa USA przeciwko Antigua i Barbuda – gry hazardowe offshore; decyzja panelu zaskarżona w WTO ( http://www.wto.org/english/tratop_e/dispu_e/distabase_wto_members1_e.htm), dokument 03-4429, sygn. WT/DS285/3 z 26/08/2003. Sprawa w toku.

3.9 Z Internetu korzystają w swej nielegalnej działalności grupy mafijne, oszuści, autorzy wirusów, piraci, szpiedzy gospodarczy i inni przestępcy. Ściganie ich nie jest łatwe, chociaż specjalne służby policji w wielu krajach starają się ich identyfikować i lokalizować, by ścigać i ukracać stwierdzone działania przestępcze; działania takie wymagają ogólnie współpracy międzynarodowej, którą należałoby silniej wspierać.

3.10 Jak zwalczać działalność przestępczą w rodzaju stron internetowych pedofilów? Zakazanie ich nie powinno stanowić żadnych trudności prawnych, należy jednak stworzyć możliwości wykrywania takich sieci. Jak z kolei chronić dzieci przed pedofilami uczestniczącymi w szczególnie popularnych wśród młodzieży dyskusjach online (tzw. czatach) w celu umówienia się na spotkanie? Dyskusji podlega nie zasadność ustanawiania zakazów i nakładania kar w poszczególnych przypadkach, ale środków, które należy wprowadzić w celu ich wprowadzenia w życie.

3.11 Dostawcy dostępu do Internetu nie są w stanie nadzorować i kontrolować wszystkich stron i wszystkich wiadomości (które stanowią korespondencję prywatną). Natomiast na żądanie właściwego organu, policji lub instytucji zajmującej się ochroną nieletnich powinni oni natychmiast wdrażać nakazy lub decyzje o zamknięciu takich stron i identyfikacji osób, które z nich korzystają; wymaga to przechowywania przez pewien czas informacji o wprowadzaniu danych do sieci oraz o połączeniach z nią.

3.12 Firmy obsługujące karty kredytowe, wyszukiwarki internetowe oraz dostawcy dostępu do Internetu powinni jednak prowadzić np. wyrywkowe kontrole służące wykrywaniu stron internetowych dla pedofilów lub oferujących inne nielegalne treści; kryteriami selekcji winny być słowa kluczowe i strefy geograficzne. O swych ustaleniach winni następnie zawiadamiać policję. Takimi samymi technikami należałoby się posługiwać do wykrywania „klientów" używających kart kredytowych do nabywania pornografii dziecięcej „na zamówienie" oraz tzw. *snuff movies* ([1]). W razie potrzeby kontrolę taką należałoby nakazać prawem. Wyszukiwarki internetowe powinny również ograniczać możliwość docierania przez internautów do pornografii dziecięcej i innych nielegalnych treści na podstawie słów i wyrażeń kluczowych.

3.13 Wymaga to również od organów publicznych zapewnienia odpowiednich środków materialnych, wykwalifikowanego personelu, współpracy transgranicznej i spójnych norm na szczeblu krajowym, europejskim i międzynarodowym, które — nie naruszając swobód internautów — umożliwią jednocześnie unieszkodliwianie jednostek i grup, korzystających z sieci do przesyłania nielegalnych treści oraz dobrowolne blokowanie dostępu niewłaściwych lub szkodliwych treści.

3.14 Jeśli walka ta ma przynieść skutek, powinna bezpośrednio objąć wszystkich użytkowników Internetu: należy ich szkolić i informować o niezbędnych środkach ostrożności umożliwiających zabezpieczenie się przed otrzymywaniem niebezpiecznych lub niepożądanych treści oraz uniemożliwiających innym wykorzystanie ich do przekazywania takich treści. Zdaniem Komitetu w części planu działania dotyczącej informacji i szkolenia pierwszeństwo należy przyznać mobilizacji użytkowników, by wzięli na siebie odpowiedzialność za samych siebie i za osoby znajdujące się pod ich opieką. Za przykład problemu posłużyć mogą internetowe strony poświęcone ochronie zdrowia, które nie podlegają żadnym regulacjom. W interesie własnego bezpieczeństwa przedsiębiorstwa powinny również prowadzić szkolenia personelu i zabezpieczyć swoje sieci i strony sprzedaży internetowej. Także i administracja oraz instytucje publiczne i prywatne powinny wprowadzać podobne zasady bezpieczeństwa i zapewnić absolutną poufność przetwarzanych danych, w szczególności danych osobowych. Kształtowaniu świadomości towarzyszyć powinno zachęcanie do korzystania z dostępnych w sieci treści wysokiej jakości oraz do zdrowych form spędzania czasu poza siecią jako alternatywy dla zbyt długiego „przesiadywania" w Internecie lub dla niektórych gier fabularnych (RPG), które na dłuższą metę mogą prowadzić do nieodwracalnych zmian osobowości u niektórych niedojrzałych graczy.

3.15 Użytkownicy powinni mieć możliwość łatwego zgłaszania nielegalnych treści, z którymi się spotkali w sieci, na specjalnych infoliniach, u odpowiednich organów lub w specjalnych służbach policyjnych, aby powiadomione w ten sposób władze publiczne mogły podjąć właściwe działania. W szczególności ostrzegać należy rodziców w krajach, w których częste jest wykorzystywanie dzieci do produkowania pornografii w sieci i na różnych nośnikach, na przykład w krajach ościennych Unii. Cel ten można wpisać do niektórych programów współpracy komisji RELEX.

3.16 Popierając konkretne cele programu — umożliwianie użytkownikom zgłaszania nielegalnych treści (infolinie), rozwój technologii filtrujących treści niepożądane, klasyfikowanie treści, zwalczanie spamu, samoregulacja przemysłu i umiejętność bezpiecznego korzystania z technologii — Komitet w uwagach szczegółowych wskazuje kilka dodatkowych celów, które uznaje za godne uwzględnienia.

## 4. **Uwagi szczegółowe Komitetu**

4.1 Komitet zwracał się już w przeszłości do Komisji o ograniczenie nadmiernej biurokracji w programach finansowanych przez UE, co umożliwiłoby między innymi dostęp do finansowania mikroprojektom lub lokalnym organizacjom pozarządowym. Komitet popiera nadzór koncentrujący się na osiąganiu wymiernych wyników w ramach tego programu oraz na skuteczności proponowanych rozwiązań. Poufność rozpowszechniania wypracowanych rozwiązań powinna być mniejsza.

4.2 Zdaniem Komitetu w ramach programu, o ile to możliwe, lub w drodze nowej inicjatywy Komisji powziąć należy działania normatywne wspierające ochronę użytkownika końcowego.

([1]) tj. filmów pokazujących prawdziwe sceny skrajnej przemocy, tortur i zabójstw.

4.3 Autorzy oprogramowania umożliwiającego dostęp do Internetu, systemów operacyjnych serwerów lub systemów zwalczania nielegalnego dostępu powinni ponosić pełną odpowiedzialność za swój produkt; użytkownicy powinni mieć gwarancję, iż autorzy takiego oprogramowania stosują najlepsze dostępne techniki i regularnie uaktualniają swoje produkty. Gwarancje takie zapewnić powinna klientom samoregulacja, a w jej braku — norma wspólnotowa.

4.4 Dostawcy dostępu do Internetu powinni udostępniać (większość z nich już to dzisiaj czyni) łatwe sposoby zwalczania wirusów już na swych stronach przed ściągnięciem poczty lub załączników oraz oferować środki wstępnego filtrowania poczty pod kątem spamu. Może to przynieść korzyści komercyjne operatorom, którzy poważnie dbają o ochronę swoich klientów. Biorąc pod uwagę fakt, iż dzieci często wyprzedzają swoich rodziców w kwestii korzystania z Internetu, systemy filtrowania poczty, usuwania wirusów, ochrony przed niepożądanymi wiadomościami i kontroli rodzicielskiej powinny być preinstalowane i łatwe w użyciu dla osób niemających szczególnej wiedzy technicznej.

4.5 Program powinien również promować badania na temat specjalistycznego oprogramowania i innych środków weryfikacji odporności kodu programów ochronnych na atak, zachęcać lub ewentualnie zmuszać dostawców do szybkiego udostępniania tzw. łat programowych likwidujących wszystkie stwierdzone lub zgłoszone niedoskonałości otwierające dostęp niepożądanym użytkownikom, do poprawy skuteczności sprzętowych i programowych rozwiązań typu firewall, jak również metod filtrowania i identyfikacji rzeczywistego pochodzenia treści.

4.6 Komitet życzyłby sobie szerszego rozpowszechnienia oceny wyników poprzedniego programu *Safer Internet*, uporządkowanych według rodzaju rozwiązywanych problemów. Należy również dbać o to, by wszystkie odsyłacze do zrealizowanych projektów pozostawały aktywne oraz by stały się szerzej znane zainteresowanym. Na stronie internetowej Komisji powinno się również informować o inicjatywach podjętych oraz doświadczeniach nabytych w państwach członkowskich i państwach trzecich, by przyczyniać się do upowszechniania wiedzy w tym zakresie i do nawiązywania pożytecznej współpracy.

4.7 W pełni możliwe jest przyjęcie aktów prawnych. Dostawcy dostępu do Internetu, firmy obsługujące karty kredytowe i wyszukiwarki internetowe mogą podlegać regulacjom prawnym, a niektóre wprowadziły już samoregulację. Sankcje karne dla stron internetowych promujących terroryzm, rasizm, samobójstwo lub pornografię dziecięcą powinny być surowe i odstraszające. należy zintensyfikować międzynarodowe działania na rzecz wykrywania i lokalizowania takich stron w celu doprowadzania do ich zamknięcia wszelkimi dostępnymi środkami względnie podejmowania zmierzających do tego negocjacji z krajami goszczącymi takie witryny.

Bruksela, 16 grudnia 2004 r.

## 5. **Podsumowanie**

Udzielając poparcia kontynuacji i rozszerzeniu programu *„Safer Internet plus”*, Komitet (który zresztą był wcześniej rzecznikiem jego uruchomienia) pragnie wyrazić pogląd, iż waga i zakres groźby nadużyć — przede wszystkim wobec dzieci — wymaga natychmiastowych i komplementarnych działań legislacyjnych i odpowiednich w poszczególnych przypadkach środków praktycznych w następujących dziedzinach:

— nałożenie na wszystkie zainteresowane podmioty powszechnego obowiązku ochrony dzieci i użytkowników w ogóle, w szczególności zaś tych najbardziej narażonych na nadużycia,

— domyślne instalowanie systemów filtrujących,

— wyraźne wiadomości ostrzegawcze na wszystkich stronach głównych i portalach dostępowych do tzw. czatów,

— wspieranie stowarzyszeń tworzących infolinie służące sygnalizowaniu stron internetowych i działalności w sieci stanowiącej poważne zagrożenie dla dzieci,

— uniemożliwienie korzystania z kart kredytowych w celu zamawiania w Internecie pornografii dziecięcej i innych nielegalnych treści, jak również w celu prania brudnych pieniędzy,

— ostrzeżenia i specjalne inicjatywy na rzecz rodziców i wychowawców, jak również władz krajów, w których wykorzystywanie dzieci do celów pornograficznych jest poważnym problemem,

— nasilenie działań zwalczających działalność wykorzystującą dzieci do celów pornograficznych powiązaną z przestępczością zorganizowaną,

— systemy identyfikujące i informujące o szkodliwych treściach oraz usuwające treści rasistowskie, rozpowszechnianie informacji na temat usiłowań popełnienia oszustw lub sprzedaży zagrażających zdrowiu substancji w Internecie w celu ochrony osób stanowiących łatwy cel lub niedoinformowanych,

— dążenie do współpracy i wspólnych zasad na szczeblu międzynarodowym w celu skuteczniejszego zwalczania spamu,

— współpraca międzynarodowa (udoskonalenie systemu wczesnego ostrzegania) i odstraszające sankcje karne dla osób rozprzestrzeniających wirusy komputerowe lub nielegalnie wykorzystujących sieci prywatne i publiczne w celach przestępczych (wtargnięcie do sieci w celu jej wykorzystania do szpiegostwa gospodarczego, zawłaszczanie częstotliwości transmisyjnych i inne szkodliwe praktyki).

*Przewodnicząca*

*Europejskiego Komitetu Ekonomiczno-Społecznego*

Anne-Marie SIGMUND