PARLAMENT EUROPEJSKI

2004 *2009*

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

2008/2160(INI)

21.1.2009

PROJEKT SPRAWOZDANIA

zawierający projekt zalecenia Parlamentu Europejskiego dla Rady w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie (2008/2160(INI))

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

Sprawozdawca: Stavros Lambrinidis

PR_INI_art114

SPIS TREŚCI

Strona

PROJEKT ZALECENIA PARLAMENTU EUROPEJSKIEGO DLA RADY 3

PROJEKT ZALECENIA DLA RADY (B6-0302/2008) 9

UZASADNIENIE 11

PROJEKT ZALECENIA PARLAMENTU EUROPEJSKIEGO DLA RADY

w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie (2008/2160(INI))

Parlament Europejski,

– uwzględniając projekt zalecenia dla Rady, przedstawiony przez Stavrosa Lambrinidisa w imieniu grupy PSE, dotyczący wzmocnienia bezpieczeństwa i podstawowych wolności w Internecie (B6-0302/2008),

– uwzględniając **Międzynarodowy pakt praw obywatelskich i politycznych**, Konwencję o ochronie praw człowieka i podstawowych wolności oraz Kartę praw podstawowych Unii Europejskiej[1], a w szczególności zawarte tam postanowienia dotyczące ochrony danych osobowych, wolności wypowiedzi, poszanowania sfery prywatnej i życia rodzinnego, jak również prawo do wolności i bezpieczeństwa,

– uwzględniając dyrektywę Parlamentu Europejskiego i Rady 95/46/WE z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych[2], ramową decyzję Rady **2008/977/WSiSW z dnia 27 listopada 2008 r.** w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych[3], dyrektywę Parlamentu Europejskiego i Rady 2003/98/WE z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego[4], wniosek Komisji dotyczący dyrektywy Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. zmieniającej dyrektywę 2002/22/WE w sprawie usługi powszechnej i praw użytkowników związanych z sieciami łączności elektronicznej, dyrektywę 2002/58/WE w sprawie przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej oraz rozporządzenie (WE) nr 2006/2004 w sprawie współpracy w zakresie ochrony konsumentów (COM(2007)0698), uwzględniając dyrektywę Parlamentu Europejskiego i Rady 2006/24/WE z dnia 15 marca 2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności[5], a także opinię rzecznika generalnego z dnia 14 października 2008 r. w sprawie C-301/06 *Irlandia v. Parlament i Rada*,

– uwzględniając ramową decyzję Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne[6], ramową decyzję Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie walki z oszustwami i fałszerstwami dotyczącymi bezgotówkowych środków płatności[7], ramową decyzję Rady **2008/919/WSiSW z dnia 28 listopada 2008 r.** zmieniającą **ramową decyzję** 2002/475/WSiSW w sprawie zwalczania

[1] Dz.U. C 364 z 18.12.2000, s. 1.
[2] Dz.U. L 281 z 23.11.1995, s. 31.
[3] Dz.U. L 350 z 30.12.2008, s. 60.
[4] Dz.U. L 345 z 31.12.2003, s. 90.
[5] Dz.U. L 105 z 21.6.2006, s. 54.
[6] Dz.U. L 69 z 16.3.2005, s. 67.
[7] Dz.U. L 149 z 2.6.2001, s. 1.

terroryzmu[1], uwzględniając komunikat Komisji z dnia 22 maja 2007 r. pt. „W kierunku ogólnej strategii zwalczania cyberprzestępczości" (COM(2007)0267), a także ostatnie inicjatywy na rzecz wykrywania ciężkiej przestępczości i terroryzmu (takie jak projekt „Check the Web"),

– uwzględniając prace prowadzone przez Radę Europy, Organizację Współpracy Gospodarczej i Rozwoju (OECD) i Organizację Narodów Zjednoczonych (ONZ) zarówno w odniesieniu do zwalczania przestępczości i przestępczości elektronicznej, jak i ochrony podstawowych praw i wolności, w tym również w Internecie[2],

– uwzględniając ostatnie orzeczenia sądów europejskich i krajowych trybunałów konstytucyjnych w tej dziedzinie, a w szczególności wyrok niemieckiego trybunału konstytucyjnego (Bundesverfassungsgericht), który uznał odrębne prawo do ochrony poufności i integralności systemów informatycznych[3],

– uwzględniając art. 114 ust. 3 i art. 94 Regulaminu,

– uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz opinię Komisji Kultury i Edukacji (A6-0000/2008),

A. mając na uwadze, że rozwój Internetu dowodzi, iż staje się on niezastąpionym narzędziem promowania inicjatyw demokratycznych, nowym forum debaty politycznej (kampanie internetowe i głosowanie drogą elektroniczną), a także kluczowym instrumentem korzystania z wolności wypowiedzi na skalę światową (pisanie blogów) oraz prowadzenia działalności gospodarczej,

B. mając na uwadze, że Internet nadaje pełne znaczenie definicji wolności wypowiedzi, zapisanej w art. 11 Karty praw podstawowych Unii Europejskiej, zwłaszcza jeżeli chodzi o jego ponadgraniczny charakter,

C. mając na uwadze, że przejrzystość, poszanowanie prywatności i atmosferę zaufania wśród zainteresowanych stron należy uważać za elementy niezbędne do powstania trwałej wizji bezpieczeństwa w Internecie,

D. mając na uwadze, że dzięki wolności, jaką gwarantuje Internet, wykorzystuje się go również jako miejsce rozpowszechniania przesłań charakteryzujących się przemocą i brakiem cech demokratycznych, takich jak nawoływanie do ataków terrorystycznych, a także mając na uwadze, że szeroko rozumiane zagrożenie przestępczością w cyberprzestrzeni, skierowane przeciwko osobom indywidualnym (w tym dzieciom) i sieciom, nasiliło się na świecie,

E. mając na uwadze, że przestępstwa te należy skutecznie i zdecydowanie zwalczać, nie

---

[1] Dz.U. L 330 z 9.12.2008, s. 21.

[2] Przykłady: konwencja Rady Europy o przestępczości w cyberprzestrzeni z dnia 23 listopada 2001 r.; konwencja Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych z dnia 28 stycznia 1981 r.

[3] BVerfG, 1 BvR 370/07, 27.2.2008, Absatz-Nr. (1 - 333). http://www.bverfg.de/entscheidungen/rs20080227_1bvr037007.html

naruszając podstaw wolnego i otwartego charakteru Internetu,

F. mając na uwadze, że w społeczeństwie demokratycznym to obywatele mają prawo obserwować i osądzać działania i opinie swoich rządów, a także prywatnych firm świadczących im usługi, a nie na odwrót – to nie rządy czy firmy mają prawo obserwować i osądzać na co dzień działania i opinie swoich obywateli oraz mając na uwadze, że technologicznie zaawansowane techniki monitorowania w połączeniu z pobłażliwym prawem określającym granice ich stosowania coraz bardziej podważają tę zasadę,

G. mając na uwadze, że gwałtowny postęp technologiczny w coraz większym stopniu pozwala na niejawne i niemożliwe do wykrycia monitorowanie poczynań obywateli w Internecie oraz mając na uwadze, że samo istnienie technologii monitoringowych nie powinno automatycznie usprawiedliwiać ich stosowania oraz mając na uwadze, że nadrzędny interes ochrony podstawowych praw obywateli powinien określać granice i dokładne okoliczności korzystania z takich technologii przez władze publiczne lub prywatne przedsiębiorstwa,

H. z uwagi na fakt, iż mając do czynienia z prawami takimi jak swoboda wypowiedzi lub poszanowanie sfery prywatnej w społeczeństwie demokratycznym, ingerencja w korzystanie z tych praw może mieć miejsce jedynie z nakazu władz publicznych, jeżeli jest zgodna z prawem, konieczna i proporcjonalna,

I. mając na uwadze, że z uwagi na swój globalny, otwarty i demokratyczny charakter Internet jest z zasady wolny, co jednak nie wyklucza potrzeby refleksji (na szczeblu krajowym i międzynarodowym, na forum publicznym i prywatnym) nad sposobem poszanowania i ochrony podstawowych swobód użytkowników Internetu i ich bezpieczeństwa,

J. mając na uwadze, że analfabetyzm elektroniczny będzie nowym rodzajem analfabetyzmu w XXI w.; mając na uwadze, że zagwarantowanie wszystkim obywatelom dostępu do Internetu oznacza wobec tego gwarancję dostępu do szkolnictwa dla wszystkich obywateli, a także mając na uwadze, że władze lub prywatne przedsiębiorstwa nie powinny takiego dostępu odmawiać; mając na uwadze, że należy koniecznie zająć się pojawiającymi się kwestiami, takimi jak neutralność sieci, interoperacyjność, globalna dostępność wszystkich połączeń internetowych oraz korzystanie z otwartych formatów i standardów,

K. mając na uwadze, że należy utrzymać właściwą równowagę między ponownym wykorzystaniem informacji sektora publicznego, co daje niespotykane możliwości eksperymentowania i wymiany w dziedzinie kreatywności i kultury, a ochroną praw do własności intelektualnej,

1. występuje do Rady z następującymi zaleceniami:

Pełny i bezpieczny dostęp do Internetu dla wszystkich

a) zaleca podejmowanie wysiłków w celu uczynienia z Internetu ważnego narzędzia wzmacniającego pozycję jego użytkowników oraz stworzenia warunków

umożliwiających rozwój inicjatyw oddolnych oraz demokracji elektronicznej przy jednoczesnym zagwarantowaniu istotnych zabezpieczeń, gdyż w dziedzinie tej mogą się pojawić nowe formy kontroli i cenzury; wolność i ochrona sfery prywatnej użytkowników Internetu powinna być rzeczywistością, a nie iluzją;

b) uznaje, że Internet może stanowić niezwykłą szansę wzmocnienia aktywnego obywatelstwa oraz że w związku z tym dostęp do sieci i treści jest jednym z kluczowych elementów; zaleca pracę nad tą kwestią w oparciu o założenie, że każdy ma prawo być częścią społeczeństwa informacyjnego oraz że instytucje i zainteresowane podmioty na wszystkich szczeblach ponoszą ogólną odpowiedzialność za wspomaganie tego rozwoju[1] oraz że należy stawić czoła dwóm nowym wyzwaniom wieku elektronicznego w postaci analfabetyzmu elektronicznego i wykluczenia z procesów demokratycznych;[2]

c) zaleca, by przy współpracy z innymi podmiotami, zadbać o nietraktowanie bezpieczeństwa, wolności wypowiedzi i prywatności, a także otwartości Internetu jako konkurujących ze sobą celów, lecz realizować je jednocześnie w ramach całościowej wizji stanowiącej stosowną odpowiedź na te wszystkie wyzwania;

Jednoznaczne zobowiązanie do zwalczania przestępczości w cyberprzestrzeni

d) zaleca zwrócenie się do prezydencji Rady i do Komisji z prośbą o refleksję się nad obszerną strategią zwalczania przestępczości w cyberprzestrzeni, w tym również nad sposobem rozwiązania problemu „kradzieży tożsamości" na szczeblu UE;

e) zachęca do refleksji na temat niezbędnej współpracy w tej dziedzinie między podmiotami publiczno-prywatnymi oraz na temat wzmocnienia współpracy dotyczącej egzekwowania prawa;

f) zaleca kontynuowanie prac podjętych w ramach projektu kontroli sieci internetowej („Check the Web") i promowanie działań mających na celu poprawę przepływu informacji na temat przestępczości w sieci, takich jak niedawne inicjatywy polegające na utworzeniu krajowych platform ostrzegawczych oraz europejskiej platformy ostrzegawczej służących rejestrowaniu wykroczeń popełnianych w Internecie, pod warunkiem że będą istnieć niezbędne zabezpieczenia;

g) zaleca wspieranie programów ochrony dzieci i kształcenia ich rodziców zgodnie z postanowieniami prawa UE w odniesieniu do nowych zagrożeń elektronicznych, a także przedstawienie oceny wpływu i skuteczności już istniejących programów;

h) zaleca przyjęcie dyrektywy w sprawie środków prawa karnego mającej na celu egzekwowanie praw do własności intelektualnej i jednocześnie, w ramach dążenia do

[1] Por. z konstytucją Grecji i jej ustępem 5A.

[2] W dokumencie Rady Europy z dnia 17 września 2008 r. na temat Internetu jako niezwykle ważnego źródła zasobów dla wszystkich zainteresowanych („Internet – a critical resource for all") podkreśla się również, że „zagwarantowanie i promowanie sprawiedliwości i partycypacji w odniesieniu do Internetu stanowi bardzo ważny krok, jeżeli chodzi o postępy w dziedzinie ogólnie pojmowanej sprawiedliwości i partycypacji w całym społeczeństwie".

realizacji tego celu, zakazującej systematycznego monitorowania i nadzoru poczynań wszystkich użytkowników Internetu oraz gwarantującej proporcjonalność kar i popełnianych wykroczeń; w związku z tym zaleca poszanowanie wolności wypowiedzi i stowarzyszania się indywidualnych użytkowników oraz zwalczanie zachęt do nadużyć w cyberprzestrzeni dotyczących praw do własności intelektualnej, w tym również pewnych nadmiernych ograniczeń dostępu wprowadzanych przez samych posiadaczy praw do własności intelektualnej;

i) domaga się gwarancji, że wyrażanie w Internecie kontrowersyjnych opinii na tematy polityczne, również w odniesieniu do terroryzmu, nie będzie podlegać odpowiedzialności karnej;

Ciągła czujność w odniesieniu do bezwzględnej ochrony i intensywnego promowania podstawowych swobód w Internecie

j) uważa, że „tożsamość cyfrowa" w coraz większym stopniu staje się integralną częścią naszego ego i w związku z tym zasługuje na stosowną i skuteczną ochronę przed ingerencją zarówno podmiotów prywatnych, jak i publicznych; zaleca zwrócenie należytej uwagi na znaczenie anonimowości, pseudonimowości i kontroli przepływu informacji dla prywatności, a także na fakt, iż użytkownicy powinni dysponować skutecznymi środkami służącymi do jej ochrony;

k) dostrzega niebezpieczeństwa, jakie kryje się w formach nadzoru i kontroli Internetu, których celem jest również śledzenie każdego „cyfrowego" kroku użytkownika oraz utworzenie na tej podstawie jego profilu i przyznanie mu „punktów"; tego rodzaju techniki należy zawsze poddawać ocenie obejmującej konieczność i proporcjonalność ich stosowania w kontekście celów, które się dzięki nim realizuje; podkreśla potrzebę głębszej świadomości i przyzwolenia użytkowników w odniesieniu do czynności podejmowanych przez nich w sieci elektronicznej (np. w przypadku społeczności internetowych);

l) zaleca zbadanie i wprowadzenie ograniczeń dotyczących „przyzwolenia", o które władze lub prywatne przedsiębiorstwa mogą się zwrócić do użytkowników lub do udzielenia którego mogą ich skłonić w celu częściowej rezygnacji z prywatności, gdyż porównanie pozycji negocjacyjnej i wiedzy użytkowników prywatnych i takich instytucji charakteryzuje się oczywistym brakiem równowagi;

m) zaleca ścisłe ograniczenie i określenie przypadków, w których organy rządowe mogą zażądać od prywatnej firmy internetowej ujawnienia danych;

n) potępia rządową cenzurę treści, których można poszukiwać w zasobach Internetu, zwłaszcza jeżeli takie ograniczenia mogłyby osłabiać wypowiedzi polityczne;

o) zaleca wezwanie państw członkowskich do zadbania o to, aby wolność wypowiedzi nie podlegała arbitralnym ograniczeniom natury publicznej lub prywatnej oraz do unikania wszelkich środków legislacyjnych lub administracyjnych, które mogłyby osłabiać wypowiedzi osób indywidualnych;

p) zwraca uwagę na fakt, że rozwój tzw. „Internetu przedmiotów" nie powinien

zepchnąć na drugi plan ochrony danych i praw obywateli;

q) zaleca promowanie zasady poszanowania prywatności od samego początku (ang. privacy by design), zgodnie z którą wymogi dotyczące prywatności i ochrony danych należy wprowadzać na jak najwcześniejszym etapie cyklu życia nowych technologii;

Przedsięwzięcia międzynarodowe

r) należy wezwać wszystkich dostawców usług internetowych do zaangażowania się w trwający proces tworzenia „internetowej karty praw", który opiera się na istniejących prawach podstawowych, wspiera ich egzekwowanie i pomaga rozpoznać kształtujące się zasady; w związku z tym dynamiczna koalicja wokół internetowej karty praw powinna odgrywać rolę przewodnią;

s) w tym kontekście należy zadbać o podjęcie inicjatywy obejmującej wiele zainteresowanych stron i wiele szczebli oraz opartej na procesie, a także o rozważenie możliwości połączenia inicjatyw globalnych i lokalnych w celu określenia i ochrony praw użytkowników Internetu, co zagwarantuje zasadność i akceptację procesu oraz odpowiedzialność zań;

t) należy zachęcać UE do aktywnego udziału w różnych forach międzynarodowych zajmujących się globalnymi i lokalnymi aspektami Internetu, takich jak Forum Zarządzania Internetem (Internet Governance Forum – IGF);

u) zaleca uczestnictwo wszystkich zainteresowanych podmiotów UE w procesie tworzenia europejskiego forum IGF, które dokonałoby bilansu doświadczeń zgromadzonych przez krajowe fora IGF, funkcjonowało jako partner na szczeblu regionalnym i skuteczniej prezentowało kwestie ogólnoeuropejskie, stanowiska i obawy w mających powstać międzynarodowych forach IGF;

o

o o

2. zobowiązuje swojego przewodniczącego do przekazania niniejszego zalecenia Radzie oraz przedstawienia go do wglądu Komisji.

11.6.2008

PROJEKT ZALECENIA DLA RADY (B6-0302/2008)

zgodnie z art. 114 ust. 1 Regulaminu

złożył Stavros Lambrinidis

w sprawie utrwalenia bezpieczeństwa i podstawowych wolności w Internecie

Parlament Europejski,

– uwzględniając europejską konwencję praw człowieka (EKPCz) i Kartę praw podstawowych, a w szczególności artykuły karty dotyczące ochrony danych osobowych, wolności słowa i informacji oraz poszanowania prywatności i życia rodzinnego,

– uwzględniając niedawne inicjatywy w sprawie wykrywania ciężkiej przestępczości i terroryzmu (projekt „Check the web") oraz niedawny wniosek dotyczący zmiany decyzji ramowej 2002/475/WSiSW Rady z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu, a także wniosku w sprawie przeglądu dyrektywy 2002/58/WE dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej,

– uwzględniając prace prowadzone przez Radę Europy, Organizację Współpracy Gospodarczej i Rozwoju (OECD) i Organizację Narodów Zjednoczonych (ONZ) zarówno w odniesieniu do zwalczania przestępczości i przestępczości elektronicznej, jak i ochrony podstawowych praw i wolności, w tym również w Internecie,

– uwzględniając ostatnie wyroki sądów europejskich i krajowych trybunałów konstytucyjnych w tej sprawie, a w szczególności wyrok niemieckiego trybunału konstytucyjnego (BVerfG), który uznał odrębne prawo do ochrony poufności i integralności systemów informatycznych,

– uwzględniając art. 114 ust. 1 Regulaminu,

A. mając na uwadze, że Internet stał się głównym narzędziem rozwoju wolności słowa i rozwijania działalności gospodarczej na świecie; mając na uwadze, że w tych okolicznościach jest sprawą absolutnie zasadniczą, aby zwalczając przestępczości i nadużycia ze strony władz publicznych i podmiotów prywatnych, nie ograniczać możliwości tego narzędzia,

B. mając na uwadze, że z uwagi na jego światowy wymiar, szybkie zmiany i szczególne cechy techniczne Internet trudno jest nadzorować w ramach samego prawa krajowego oraz że zwłaszcza na gruncie międzynarodowym należy podjąć inicjatywy na rzecz ochrony praw osób prywatnych zarówno dotyczących ich bezpieczeństwa, jak i chroniących wolności oraz prywatność,

1. występuje do Rady z następującymi zaleceniami:

   a) należy umożliwić stopniowe zbliżanie ustawodawstwa krajowego w UE, które dotyczy wymogów związanych z ochroną praw podstawowych w Internecie;

   b) należy umocnić dialog między legislacyjnymi organami krajowymi i europejskimi oraz między krajowym i europejskim wymiarem sprawiedliwości;

   c) należy wspierać dialog między wszystkimi zaangażowanymi podmiotami, których dotyczy zjawisko Internetu, w szczególności dostawcami Internetu i użytkownikami;

   d) należy wspierać zawieranie niezbędnych umów na szczeblu międzynarodowym, zarówno w stosunkach dwustronnych (w szczególności w stosunkach transatlantyckich), jak i wielostronnych (inicjatywy Rady Europy, OECD i ONZ);

2. zobowiązuje swojego przewodniczącego do przekazania niniejszego zalecenia Radzie oraz przedstawienia go do wglądu Komisji.

UZASADNIENIE

Prawa podstawowe w Internecie – poprawa sytuacji i zagrożenia

Żyjemy w czasach, w których każdy od władz po policję, przedsiębiorstwa prywatne, a nawet przestępców, poszukuje możliwie najpełniejszego dostępu do naszych prywatnych danych elektronicznych. W szczególności Internet oferuje niegdyś niewyobrażalny dostęp do szczegółów naszego życia prywatnego; nawet zwykłe kliknięcie myszką w obrębie strony internetowej generuje dane, które potencjalnie mogą być użyte lub nadużywane przez osoby zajmujące się marketingiem, służby wywiadowcze lub złodziei tożsamości.

Dlatego zagwarantowanie ochrony **podstawowego prawa do prywatności** w Internecie jest jednym z najpilniejszych zadań, postawionych przed nami jako prawodawcami. Jest to również jedno z najtrudniejszych wyzwań etycznych, prawnych, technicznych i politycznych, z jakimi kiedykolwiek spotkało się nasze społeczeństwo.

Dla wszystkich jest jasnym, że Internet może być narzędziem poszerzającym zakres naszych praw podstawowych, dostarczając nam nieograniczonych informacji oraz angażując nas w życie zarówno jednostek jak i społeczności na całym świecie. Jednak z jakiegoś powodu znacznie mniejszą uwagę przywiązuje się do faktu, że Internet stanowi ogromne zagrożenie dla naszych praw podstawowych, potencjalnie wystawiając nas na zgubną inwigilację, jednocześnie służąc jako narzędzie przestępcom, a nawet terrorystom. Najtrudniej jest ująć Internet w ramy prawne w taki sposób, aby korzystać z jego zalet przy jednoczesnym ograniczaniu bardzo realnych i poważnych zagrożeń związanych z jego nadużywaniem. Właściwą ocenę komplikuje szczególny charakter Internetu, będącego zdecentralizowaną, zarządzaną przez użytkownika siecią, której nie kontroluje żadna władza i która pokonuje prawie wszystkie granice.

Z tego względu celem niniejszego sprawozdania jest zwrócenie większej uwagi na metody ochrony oraz promowania podstawowych wolności jednostek online. Wśród najważniejszych elementów naszej reakcji na tę sytuację powinny się znaleźć:

– zaangażowanie wszystkich zainteresowanych stron;
– działania na wielu szczeblach, wykorzystywanie istniejących krajowych, regionalnych i międzynarodowych instrumentów oraz obserwowanie, w jaki sposób są one stosowane we współczesnej praktyce legislacyjnej;
– wymiana sprawdzonych wzorców postępowania; oraz
– odpowiedź na potrzeby i problemy różnego rodzaju użytkowników Internetu oraz związane z wieloma (wciąż rozwijającymi się) rodzajami czynności podejmowanych online.

Nasze działania skupiają się na uzyskaniu odpowiedniej równowagi pomiędzy prywatnością a bezpieczeństwem. Będzie to wymagać ciągłej kontroli oraz dostosowań, pozwalających dotrzymać kroku niepohamowanemu rozwojowi technologii. Należy uważnie rozważyć kwestie związane z bezpieczeństwem wszelkiego rodzaju, od bezpieczeństwa narodowego po bezpieczeństwo i niezawodność naszych sieci, osobiste bezpieczeństwo jednostek, gdy dzielą się swoimi danymi w sieci. Jeżeli zapewnienie bezpieczniejszego Internetu jest uzasadnionym celem dla naszych społeczeństw, należy zająć się kwestią technik inwigilacji i monitoringu

oraz ograniczyć takie praktyki, ponieważ mogą one zagrażać naszym podstawowym wolnościom, szczególnie jeżeli chodzi o konieczność ich stosowania, ich proporcjonalność oraz skuteczność. Elastyczność, łatwość dostosowywania oraz niezawodność powinny być cechami charakterystycznymi wszelkich przepisów oraz programów, nad którymi pracujemy, pozwalając nam zawsze o krok wyprzedzić rozwijającą się technologię.

Internet może również w znaczny sposób wpłynąć na poprawę innych praw podstawowych takich jak wolność wypowiedzi, wolność działalności politycznej i zrzeszania się, w równie łatwy jednak sposób może te prawa podkopywać. Ostatnio poddano debacie inicjatywę legislacyjną dotyczącą monitorowania wypowiedzi w Internecie, której celem było przeciwdziałanie atakom terrorystycznym. Jest to klasyczny przykład prawa, które jeżeli nie jego założenia nie zostaną precyzyjnie zdefiniowane, może otworzyć furtkę inwigilacji na skalę masową, „studząc" polityczne wypowiedzi jednostek, które leżą u podstaw demokratycznego społeczeństwa.

Istotne jest znalezienie równowagi w kwestiach takich jak ta. Nie ulega wątpliwości, że Internet wyposażył przestępców w zbiór nowych narzędzi i oczywistym jest, że terroryści nie powinni mieć możliwości wykorzystywania Internetu do planowania i przeprowadzania ataków. Jednocześnie społeczeństwa słusznie domagają się wyplenienia pornografii dziecięcej w Internecie. Tacy przestępcy, stanowiąc wymierne zagrożenie, zmniejszają opór obywateli związany z apelami policji o szeroko zakrojone monitorowanie Internetu, który ze swej natury jest „nietrwały". Nie wolno nam pójść w tę stronę. Przepisy prawa muszą być skuteczne w zwalczaniu przestępczości, jednak nie mogą regulować zbyt wiele. Internet, ze względu na swoją nieuchwytną i niewymierną naturę jest podatny na takie nadużycia. Na przykład niewiele osób mogłoby zaakceptować sytuację, w której policja czy firmy marketingowe mogłyby otwierać każdy list wysłany drogą pocztową w celu sprawdzenia jego treści. Podobna czujność jest nieodzowna w przypadku ochrony treści wiadomości elektronicznych.

Jednak nie tylko władze publiczne mogą, w swej pogoni za przestępcami, ostudzić zagorzałość wypowiedzi, czy naruszyć prywatność, robią to także prywatne przedsiębiorstwa Internetowe w pogoni za zyskiem. Według najnowszych trendów, gdy to się wyda – a zazwyczaj po tym jak przedsiębiorstwa zostały złapane na gorącym uczynku gromadząc, przechowując oraz wykorzystując nasze dane bez autoryzacji – wymaga się „**zgody"** użytkownika (na zasadzie wyboru) na używanie jego lub jej danych.

Należy zadać sobie pytanie: **„Jakie są granice takiej zgody?"** Pytanie to dotyczy zarówno danych, o ujawnienie których dane przedsiębiorstwo może poprosić użytkownika jak również tego, co osoba prywatna powinna móc ujawnić, jeśli chodzi o swoją prywatność oraz w zakresie innych praw podstawowych w celu otrzymania danej usługi Internetowej lub przywileju w Internecie.

Odpowiedzi na te pytania nie są proste. W innym obszarze – w zakresie prawa pracy – nasze społeczeństwa uzgodniły granice zgody obywatela, jeżeli chodzi o jego życie prywatne. Prawo pracy oraz układy zbiorowe w większości państw członkowskich definiują na przykład maksymalny czas pracy, pensję minimalną oraz inne uprawnienia pracowników, których pracodawca nie może z nimi negocjować. Powód jest prosty: zakłada się, że nie istnieje równowaga sił pomiędzy pracodawcą a pracownikiem oraz że w konsekwencji, nie można by

wyrazić lub wymagać „zgody” na uczciwych zasadach. Inny powód to fakt, że zdecydowaliśmy się ograniczać zmniejszanie wszelkich uprawnień pracowników, co mogłoby mieć miejsce gdyby mogli oni indywidualnie negocjować niektóre ze swoich praw, lub byli zmuszani do ich negocjowania.

Na podobne nadużycia pozwala nam Internet, biorąc pod uwagę niedoinformowanie jego użytkowników. Władza, wiedza oraz interesy władz publicznych i przedsiębiorstw prywatnych wygrywają z użytkownikiem indywidualnym, tak samo jak niebezpieczeństwo związane z oferowanymi tańszymi, a tym samym atrakcyjniejszymi dla pewnych użytkowników, usługami internetowymi w zamian za mniejszą ochronę prywatności. Sprawozdawca wyraża przekonanie, że kolejna batalia w debacie na temat bezpieczeństwa i prywatności w Internecie zostanie stoczona na temat granic „zgody” wymaganej przez władze publiczne i przedsiębiorstwa prywatne.

Ta kwestia powinna być nam szczególnie bliska, ponieważ w dzisiejszej Europie „wielki brat” nie przybiera formy autorytarnego reżimu: Jeżeli w ogóle przychodzi, to przychodzi po cichu i za naszym „przyzwoleniem”.

Co więcej **prawo do kształcenia oraz prawo do dostępu do Internetu** to dwa dodatkowe prawa, które należy promować same w sobie, choć mogą one być zagrożone w kontekście zwalczania przestępczości w cyberprzestrzeni. Analfabetyzm elektroniczny będzie nowym rodzajem analfabetyzmu w XXI w. Ponieważ każde dziecko w dzisiejszych czasach ma prawo do edukacji, a każdy dorosły do jej kontynuowania, każda osoba przez całe życie winna posiadać prawo do dostępu do komputera i do Internetu. Władze powinny zapewnić taki dostęp nawet w najbardziej oddalonych regionach, jak również najbiedniejszym obywatelom; Zakaz dostępu do Internetu nie powinien stanowić kary wymierzanej obywatelom za naruszenie przepisów. Każdy człowiek, niezależnie od stylu życia, regionu czy kultury powinien mieć możliwość czerpania korzyści z szerokiego wachlarza usług oferowanych za pośrednictwem Internetu. W ten sposób osoby te mogą się rozwijać, angażować w relacje zawodowe, osobiste i związane z edukacją oraz stwarzać maksimum możliwości gospodarczych, przy zastosowaniu technologii i poszanowaniu przepisów.