

Utrwalenie bezpieczeństwa i podstawowych wolności w Internecie

Zalecenie Parlamentu Europejskiego z dnia 26 marca 2009 r. 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, 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 danych¹, 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 karnych², dyrektywę Parlamentu Europejskiego i Rady 2003/98/WE z dnia 17 listopada 2003 r. w sprawie ponownego wykorzystywania informacji sektora publicznego³, 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 łączności⁴, a także wyrok Trybunału Sprawiedliwości Wspólnot Europejskich z dnia 10 lutego 2009 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 informatyczne⁵, ramową decyzję Rady 2001/413/WSiSW z dnia 28 maja 2001 r. w sprawie walki z oszustwami i fałszerstwami dotyczącymi bezgotówkowych środków płatności⁶, ramową decyzję Rady 2008/919/WSiSW z dnia 28 listopada 2008 r.

¹ Dz.U. L 281 z 23.11.1995, s. 31.

² Dz.U. L 350 z 30.12.2008, s. 60.

³ Dz.U. L 345 z 31.12.2003, s. 90.

⁴ Dz.U. L 105 z 13.4.2006, s. 54.

⁵ Dz.U. L 69 z 16.3.2005, s. 67.

⁶ Dz.U. L 149 z 2.6.2001, s. 1.

zmieniającą ramową decyzję 2002/475/WSiSW w sprawie zwalczania terroryzmu¹, 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 Internecie²,
 - 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 informatycznych³,
 - uwzględniając art. 114 ust. 3 i art. 94 Regulaminu,
 - uwzględniając sprawozdanie Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych oraz opinię Komisji Kultury i Edukacji (A6-0103/2009),
- 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, jak również mechanizmem służącym wspieraniu umiejętności informatycznych i rozpowszechnianiu wiedzy (e-learning), mając na uwadze, że Internet zapewnia osobom ze wszystkich grup wiekowych większe możliwości komunikowania się z ludźmi z różnych części świata, ułatwiając zapoznanie się z innymi kulturami, a co za tym idzie zrozumienie innych ludzi i kultur; mając na uwadze, że Internet zwiększył także różnorodność źródeł informacji dostępnych dla obywateli, którzy obecnie mogą zapoznawać się z informacjami z różnych części świata,
- B. mając na uwadze, że rządy oraz organizacje i instytucje interesu publicznego powinny zapewnić właściwe ramy regulacyjne i odpowiednie środki techniczne, aby umożliwić obywatelom czynny i skuteczny udział w procedurach administracyjnych za pośrednictwem usług administracji elektronicznej,
- C. mając na uwadze, że Internet nadaje pełne znaczenie definicji swobody wypowiedzi, zapisanej w art. 11 Karty praw podstawowych Unii Europejskiej, zwłaszcza jeżeli chodzi o pokonywanie granic,
- D. 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,

¹ Dz.U. L 330 z 9.12.2008, s. 21.

² Np.: 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.

- E. mając na uwadze, że w Internecie wolność wypowiedzi i prywatność mogą być zwiększone, jak i bardziej narażone na ingerencje i ograniczenia ze strony podmiotów prywatnych i publicznych,
- F. mając na uwadze, że dzięki wolności, jaką gwarantuje Internet, wykorzystuje się go również jako miejsce rozpowszechniania przesłań charakteryzujących się przemocą, takich jak nawoływanie do ataków terrorystycznych, jak również tworzenie stron internetowych, które mogą wyraźnie prowokować do opartych na nienawiści działań przestępczych, 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,
- G. mając na uwadze, że przestępstwa te należy skutecznie i zdecydowanie zwalczać, nie naruszając podstaw wolnego i otwartego charakteru Internetu,
- H. 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 oraz mając na uwadze, że technologicznie zaawansowane techniki monitorowania, niejednokrotnie w połączeniu z brakiem odpowiednich gwarancji prawnych dotyczących granic ich stosowania, coraz bardziej podważają tę zasadę,
- I. mając na uwadze, że jednostki mają prawo do swobodnej wypowiedzi w Internecie (np. za pomocą treści tworzonych przez użytkowników, blogów, społeczności internetowych); mając również na uwadze, że dzięki wyszukiwarkom i dostawcom usług internetowych uzyskanie informacji na przykład o innych osobach stało się znacznie łatwiejsze; mając jednak na uwadze, że w niektórych sytuacjach jednostki chciałyby usunąć informacje przechowywane w takich bazach danych; mając zatem na uwadze, że przedsiębiorstwa muszą być w stanie zagwarantować możliwość usunięcia danych osobowych z baz danych,
- J. mając na uwadze, że gwałtowny postęp technologiczny w coraz większym stopniu pozwala na niejawne monitorowanie poczynań obywateli w Internecie, niemożliwe do wykrycia przez jednostkę, oraz mając na uwadze, że samo istnienie technologii monitoringowych nie usprawiedliwia automatycznie 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 przedsiębiorstwa; mając na uwadze, że zwalczanie przestępczości internetowej i zagrożeń dla otwartego społeczeństwa demokratycznego stwarzanych przez osoby i organizacje wykorzystujące Internet, by narazić na szwank prawa obywateli, nie może oznaczać, że państwa członkowskie mogą przypisywać sobie prawo do przechwytywania i monitorowania całego przesyłu danych w Internecie mającego miejsce na ich terytorium, niezależnie od tego, czy dotyczy to ich własnych obywateli, czy przesyłu danych z zagranicy; mając na uwadze, że zwalczanie przestępczości musi być proporcjonalne do charakteru przestępstw,
- K. mając na uwadze, że kradzież tożsamości i oszustwa dotyczące tożsamości stanowią rosnący problem, z którego władze, indywidualni obywatele i firmy dopiero zaczynają zdawać sobie sprawę, co powoduje poważne obawy dotyczące bezpieczeństwa w odniesieniu do nasilającego się wykorzystywania Internetu do wielu celów, w tym handlu poufnymi informacjami i ich wymiany,
- L. z uwagi na fakt, iż mając do czynienia z prawami takimi jak swoboda wypowiedzi lub poszanowanie sfery prywatnej, ograniczenia w korzystaniu z tych praw mogą mieć miejsce

z nakazu władz publicznych, jeżeli są zgodne z prawem, konieczne, proporcjonalne i właściwe w społeczeństwie demokratycznym,

- M. mając na uwadze, że w Internecie istnieje przepaść uprawnień i wiedzy pomiędzy firmami i instytucjami rządowymi z jednej strony a indywidualnymi użytkownikami z drugiej strony; mając na uwadze, że w związku z tym należy zainicjować debatę na temat niezbędnych granic „zgody”, zarówno w odniesieniu do danych, o których ujawnienie przedsiębiorstwa i rządy mogą zwrócić się do użytkownika, jak i tego, ile osoba prywatna powinna być zobowiązana ujawnić ze swojej prywatności oraz w zakresie innych praw podstawowych w celu otrzymania pewnych usług internetowych lub innych przywilejów,
- N. 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, jak również na forum publicznym i prywatnym) nad sposobem poszanowania i ochrony podstawowych swobód użytkowników Internetu i ich bezpieczeństwa,
- O. mając na uwadze, że wśród licznych praw podstawowych naruszanych w świecie Internetu znajdują się m.in. poszanowanie prywatności (w tym prawo do trwałego usunięcia osobistego śladu cyfrowego), ochrony danych, wolności wypowiedzi, słowa i zrzeszania się, wolności prasy, wypowiedzi politycznej i udziału, niedyskryminacji i kształcenia; mając na uwadze, że treść takich praw, w tym ich obszar zastosowania i zakres, zapewniany poziom ochrony oraz zakaz ich naruszania powinny regulować przepisy dotyczące ochrony praw człowieka i praw podstawowych zagwarantowane w konstytucjach państw członkowskich, umowach międzynarodowych dotyczących praw człowieka, w tym Konwencji o ochronie praw człowieka i podstawowych wolności, oraz ogólne zasady prawa wspólnotowego i Karty praw podstawowych Unii Europejskiej i/lub inne właściwe przepisy prawa krajowego, międzynarodowego i wspólnotowego w ramach ich obszarów zastosowania,
- P. mając na uwadze, że wszystkie podmioty zaangażowane i aktywne w Internecie powinny przyjąć na siebie spoczywającą na nich odpowiedzialność i zaangażować się na forach, gdzie omawiane są ważne i niecierpiące zwłoki kwestie odnoszące się do działalności w Internecie, aby szukać wspólnych rozwiązań i promować je,
- Q. 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 dostępu takiego nie należy nadużywać w ramach działalności sprzecznej z prawem; 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,
- R. mając na uwadze, że infrastruktura techniczna i protokoły internetowe nie wspierają jeszcze w pełni międzynarodowego, wielokulturowego, a zwłaszcza wielojęzycznego charakteru Internetu,
- S. mając na uwadze, że w trwającym procesie związanym z „Internetową kartą praw” jest istotne, aby wziąć pod uwagę wszystkie właściwe badania i przedsięwzięcia w tej

dziedzinie, w tym ostatnie badania Unii na ten temat¹,

- T. mając na uwadze, że działalność gospodarcza jest ważna dla dalszego dynamicznego rozwoju Internetu, a zapewnienie jej opłacalności wymaga uczciwej konkurencji i ochrony praw własności intelektualnej, zgodnie z wymogiem konieczności, proporcjonalności i adekwatności,
- U. 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,
- V. mając na uwadze, że na całym świecie rządy wywierają coraz większą presję na przedsiębiorstwa z sektora technologii informacyjno-komunikacyjnych (ICT), wymagając przestrzegania krajowych przepisów i polityk w sposób, który może być sprzeczny z uznanymi na szczeblu międzynarodowym prawami człowieka, jakimi są wolność wypowiedzi i ochrona prywatności; mając na uwadze, że podjęto konstruktywne działania, między innymi przez grupę złożoną z wielu zainteresowanych stron, w tym przedsiębiorstw, organizacji społeczeństwa obywatelskiego (między innymi grup działających na rzecz praw człowieka i wolności prasy), inwestorów i przedstawicieli środowisk naukowych, która opracowała podejście oparte na współpracy mające na celu ochronę i zwiększanie wolności wypowiedzi i ochronę prywatności w sektorze ITC oraz utworzyła inicjatywę „Global Network Initiative” (GNI)²,
- W. mając na uwadze, że rygorystyczne przepisy dotyczące ochrony danych leżą w sferze zainteresowań UE i jej obywateli, a punkt 2 preambuły dyrektywy 95/46/WE dotyczącej ochrony danych wyraźnie stanowi, że rozwiązania technologiczne (tzn. systemy przetwarzania danych) „są tworzone po to, aby służyły człowiekowi” i muszą „szanować ich podstawowe prawa i wolności, szczególnie prawo do prywatności, oraz przyczyniać się do postępu gospodarczego i społecznego, rozwoju handlu oraz dobrobytu jednostek”,

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 niezwykle 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

¹ Ostatnie badanie zatytułowane „Zwiększenie bezpieczeństwa i podstawowych swobód w sieci - polityka UE na rzecz walki z cyberprzestępczością” proponuje między innymi przyjęcie niewiążącej Internetowej karty praw.

² <http://www.globalnetworkinitiative.org/index.php>.

szczeblach ponoszą ogólną odpowiedzialność za wspomaganie tego rozwoju oraz że należy stawić czoła dwóm nowym wyzwaniom wieku elektronicznego w postaci analfabetyzmu elektronicznego i wykluczenia z procesów demokratycznych¹;

- c) apeluje do państw członkowskich, aby zareagowały na rosnące zapotrzebowanie społeczeństwa na informacje i znalazły sposoby zapewnienia większej przejrzystości w procesie decyzyjnym poprzez zwiększenia dostępu obywateli do informacji przechowywanych przez rządy w celu umożliwienia obywatelom wykorzystania tych informacji; wzywa do stosowania tej samej zasady w odniesieniu do posiadanych przez nią informacji;
- d) zaleca, by przy współpracy z innymi podmiotami, zadbać o nietraktowanie bezpieczeństwa, wolności wypowiedzi i ochrony 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;
- e) domaga się gwarancji, że przysługujące nieletnim środki ochrony, zapisane w Konwencji ONZ o prawach dziecka i odzwierciedlone w prawodawstwie UE, znajdują pełne odzwierciedlenie we wszystkich właściwych działaniach, instrumentach i decyzjach odnoszących się do wzmocnienia bezpieczeństwa i wolności w Internecie;

Jednoznaczne zobowiązanie do zwalczania przestępczości w cyberprzestrzeni

- f) wzywa prezydencję Rady i państwa członkowskie do rozważenia i opracowania kompleksowej strategii na rzecz zwalczania cyberprzestępczości, zgodnie między innymi z konwencją Rady Europy w sprawie cyberprzestępczości, uwzględniającej sposoby rozwiązania problemu kradzieży tożsamości i oszustw na szczeblu UE we współpracy zarówno z dostawcami usług internetowych, jak i z organizacjami użytkowników, a także z organami policji zajmującymi się przestępczością informatyczną oraz do przedłożenia wniosku dotyczącego sposobu tworzenia kampanii informacyjnych i zapobiegania takiej przestępczości przy jednoczesnym zapewnianiu, by użytkowanie Internetu było bezpieczne i nieodpłatne dla ogółu użytkowników; wzywa do utworzenia unijnego działu pomocy ofiarom kradzieży tożsamości i oszustw dotyczących tożsamości;
- g) zachęca do refleksji na temat niezbędnej współpracy w tej dziedzinie między podmiotami publiczno-prywatnymi oraz na temat wzmocnienia współpracy dotyczącej egzekwowania prawa, wraz z odpowiednim szkoleniem dla organów ścigania i wymiaru sprawiedliwości, w tym szkoleniem na temat ochrony praw podstawowych; uznaje potrzebę wspólnej odpowiedzialności oraz korzyści ze współregulacji i samoregulacji stanowiących skuteczną alternatywę lub instrumenty uzupełniające w stosunku do tradycyjnego prawodawstwa;
- h) zaleca zapewnienie, by prace podjęte w ramach projektu kontroli sieci internetowej („Check the Web”) i niedawne inicjatywy mające na celu poprawę przepływu informacji na temat przestępczości w sieci, w tym poprzez utworzenie krajowych platform ostrzegawczych oraz europejskiej platformy ostrzegawczej służących rejestrowaniu

¹ 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”.

wykroczeń popełnianych w Internecie (utworzenie europejskiej platformy poświęconej przestępczości w sieci przez Europol), były konieczne, proporcjonalne i właściwe, a także by towarzyszyły im wszelkie niezbędne zabezpieczenia;

- i) wzywa państwa członkowskie do dokonania aktualizacji ustawodawstwa dotyczącego ochrony osób niepełnoletnich korzystających z Internetu, przede wszystkim poprzez wprowadzenie kar za przestępstwo uwodzenia dzieci przez Internet (tzw. „grooming”), zgodnie z definicją zapisaną w konwencji Rady Europy z dnia 25 października 2007 r. o ochronie dzieci przed seksualnym wykorzystywaniem i niegodziwym traktowaniem w celach seksualnych;
- j) 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; w działaniach tych szczególnie nacisk należy kłaść na gry internetowe, które skierowane są przede wszystkim do dzieci i młodzieży;
- k) zachęca wszystkich producentów komputerów z UE do fabrycznego instalowania łatwego aktywacji oprogramowania służącego ochronie dzieci;
- l) zaleca przyjęcie dyrektywy w sprawie środków prawa karnego mającej na celu egzekwowanie praw do własności intelektualnej, w oparciu o ocenę zasadności i proporcjonalności dyrektywy w świetle współczesnych badań w zakresie innowacyjności, i jednocześnie, w ramach dążenia do 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;
- m) domaga się gwarancji, że wyrażanie w Internecie kontrowersyjnych opinii na tematy polityczne nie będzie podlegało odpowiedzialności karnej;
- n) zaleca zapewnienie, by prawo dziennikarzy i mediów do zbierania i rozpowszechniania informacji dla celów informowania opinii publicznej nie było ograniczane, a jego wykonywanie nie podlegało karze zgodnie z jakimikolwiek przepisami lub stosowanymi praktykami;

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

- o) 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 – tym samym należy określić i chronić zbiór danych właściwych „tożsamości cyfrowej” osoby, a wszystkie jego elementy należy uznać za niezbywalne prawa osobiste i nieekonomiczne; 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 oraz wiedzą na ich temat, na przykład dzięki różnym dostępnym technologiom na rzecz ochrony prywatności (PET);

- p) zaleca zapewnienie, że państwa członkowskie, które przechwytyją dane i monitorują ich przepływ – bez względu na to, czy mowa o przepływie danych dotyczących ich obywateli, czy o przepływie danych z zagranicy - robią to stosując się ścisłych warunków i środków ostrożności przewidzianych przez prawo; zaleca wezwanie państw członkowskich do zapewnienia, by przeszukiwanie zdalne, o ile przewidziane prawem krajowym, prowadzono w oparciu o ważny nakaz przeszukania wydany przez właściwe władze sądowe; należy zauważyć, że uproszczone procedury przeszukiwania zdalnego w porównaniu z przeszukiwaniem bezpośrednim są niedopuszczalne, gdyż naruszają zasadę państwa prawa i prawo do prywatności;
- q) dostrzega niebezpieczeństwo, jakie kryje się w niektórych 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, związanych z wymianą danych osobowych (np. w przypadku społeczności internetowych);
- r) wzywa państwa członkowskie do zidentyfikowania wszystkich podmiotów nadzorujących sieć oraz do przygotowania powszechnie dostępnego sprawozdania rocznego w sprawie nadzoru sieci przy zagwarantowaniu zgodności z prawem, proporcjonalności i przejrzystości;
- s) 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;
- t) zaleca ściśle ograniczenie, określenie i uregulowanie przypadków, w których organy rządowe mogą zażądać od prywatnej firmy internetowej ujawnienia danych, oraz dodatkowe zapewnienie, by ich wykorzystywanie przez rządy podlegało najściślejszym standardom ochrony danych; zaleca ustanowienie skutecznej kontroli i oceny tego procesu;
- u) podkreśla znaczenie umożliwienia użytkownikom Internetu zwiększenia ich prawa do nieodwracalnego usunięcia ich danych osobowych umieszczonych na stronach internetowych lub jakichkolwiek nośnikach danych osób trzecich; zaleca zagwarantowanie, że dostawcy usług internetowych, dostawcy usług e-handlu oraz usług społeczeństwa informacyjnego uszanują decyzje użytkowników; zaleca, aby państwa członkowskie zagwarantowały skuteczne egzekwowanie prawa obywateli do dostępu do ich danych osobowych, w tym, w stosownych przypadkach, do wykreślenia takich danych lub ich usunięcia ze stron internetowych;
- v) potępia rządową cenzurę treści, których można poszukiwać w zasobach Internetu, zwłaszcza jeżeli takie ograniczenia mogłyby osłabiać wypowiedzi polityczne;
- w) 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 wolność słowa we wszelkich jej przejawach;

- x) przypomina, że transfer danych osobowych do krajów trzecich musi się odbywać zgodnie z postanowieniami między innymi dyrektywy 95/46/WE oraz decyzji ramowej 2008/977/WSiSW;
- y) zwraca uwagę na fakt, że rozwój tzw. „Internetu przedmiotów” i wykorzystywanie systemów identyfikacji radiowej (RFID) nie powinny zepchnąć na drugi plan ochrony danych i praw obywateli;
- z) zaleca wezwanie państw członkowskich do właściwego stosowania dyrektywy 95/46/WE w sprawie danych osobowych w odniesieniu do Internetu; zaleca przypomnienie państwom członkowskim, że dyrektywa ta, a w szczególności art. 8, ma zastosowanie bez względu na rodzaj technologii wykorzystywanej do przetwarzania danych osobowych oraz że w dyrektywie tej wzywa się państwa członkowskie do zapewnienia prawa do korzystania ze środków prawnych i odszkodowania za naruszenie jej przepisów (art. 22, 23 i 24);
- aa) zaleca włączenie podstawowych zasad „internetowej karty praw” do procesu badawczo-rozwojowego dotyczącego narzędzi i programów związanych z Internetem oraz 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, celem zapewnienia korzystnego środowiska obywatelom jako użytkownikom;
- ab) zaleca wspieranie i postulowanie czynnego uczestnictwa Europejskiego Inspektora Ochrony Danych i Grupy Roboczej Art. 29 w opracowywaniu wspólnotowego prawodawstwa dotyczącego działalności internetowej o potencjalnym wpływie na ochronę danych;

Przedsięwzięcia międzynarodowe

- ac) 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;
- ad) 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;
- ae) przyznaje, że globalny i otwarty charakter Internetu wymaga globalnych standardów ochrony danych, bezpieczeństwa i wolności słowa; w tym kontekście wzywa państwa członkowskie do podjęcia inicjatywy na rzecz opracowania takich standardów; z zadowoleniem przyjmuje rezolucję w sprawie pilnej potrzeby chronienia prywatności w świecie bez granic i opracowania wspólnego wniosku celem ustalenia międzynarodowych standardów ochrony prywatności i danych osobowych, przyjętego na 30. międzynarodowej konferencji rzeczników ochrony danych i prywatności zorganizowanej w Strasburgu, w dniach 15-17 października 2008 r.; zaleca wezwanie wszystkich zainteresowanych podmiotów z UE (prywatnych, jak i państwowych) do uczestnictwa w tych rozważaniach;

- af) zaleca podkreślenie znaczenia utworzenia prawdziwej internetowej e-agory, w ramach której obywatele państw Unii mogą prowadzić bardziej interaktywną dyskusję z podmiotami stanowiącymi prawo i innymi zainteresowanymi podmiotami instytucjonalnymi;
- ag) 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);
- ah) 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.