Parlament Europejski
2014-2019

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

2015/2147(INI)

01.12.2015

OPINIA

Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

dla Komisji Przemysłu, Badań Naukowych i Energii oraz Komisji Rynku Wewnętrznego i Ochrony Konsumentów

w sprawie „W kierunku aktu o jednolitym rynku cyfrowym”
(2015/2147(INI))

Sprawozdawca komisji opiniodawczej (*): Michał Boni

(*) Zaangażowana komisja – art. 54 Regulaminu

WSKAZÓWKI

Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych zwraca się do Komisji Przemysłu, Badań Naukowych i Energii oraz Komisji Rynku Wewnętrznego i Ochrony Konsumentów, jako komisji przedmiotowo właściwych, o uwzględnienie w końcowym tekście projektu rezolucji następujących wskazówek:

1. podkreśla konieczność zachowania zgodności wszystkich inicjatyw realizowanych w ramach Strategii jednolitego rynku cyfrowego dla Europy z prawami podstawowymi, w szczególności z przepisami w dziedzinie ochrony danych, uznając jednocześnie dodatkowe korzyści tej strategii dla gospodarki UE; podkreśla fakt, że poszanowanie praw podstawowych, w szczególności prywatności i ochrony danych osobowych to kluczowe elementy procesu budowania zaufania i bezpieczeństwa obywateli, które są niezbędne w rozwoju gospodarki opartej na danych w celu wykorzystania potencjału sektora cyfrowego; należy zatem uznać, że stwarzają one możliwości i przewagę konkurencyjną; podkreśla potrzebę współdziałania technologii, przedsiębiorstw i organów publicznych, aby zapewnić zgodność z obowiązującymi w UE przepisami; przypomina o znaczeniu szybkiego przyjęcia zarówno ogólnego rozporządzenia o ochronie danych, jak i dyrektywy o ochronie danych, co będzie w interesie zarówno podmiotów danych, jak i przedsiębiorstw; apeluje o przegląd dyrektywy o prywatności i łączności elektronicznej, aby zapewnić spójność przepisów z pakietem dotyczącym ochrony danych przed wejściem w życie tego pakietu;

3.3.2. Zwalczanie nielegalnych treści w internecie

2. wzywa Komisję dokonania postępów w polityce i ramach prawnych dotyczących zwalczania cyberprzestępczości oraz nielegalnych treści i materiałów w internecie, w tym mowy nienawiści, które będą w pełni zgodne z prawami podstawowymi określonymi w Karcie praw podstawowych Unii Europejskiej, a zwłaszcza z prawem do wolności słowa i swobodnego dostępu do informacji, z obowiązującym prawem UE i ustawodawstwem państw członkowskich, a także z zasadami konieczności, proporcjonalności, sprawiedliwości proceduralnej i państwa prawa; jest zdania, że aby osiągnąć ten cel, należy:
   - zapewnić europejskim i krajowym służbom policyjnym i organom ścigania spójne i skuteczne narzędzia egzekwowania prawa;
   - zapewnić jasne wytyczne określające, jak postępować z nielegalnymi treściami internetowymi, w tym z mową nienawiści;
   - wspierać partnerstwa publiczno-prywatne i dialog między podmiotami publicznymi i prywatnymi, zgodnie z obowiązującymi przepisami UE;
   - doprecyzować rolę pośredników oraz platform internetowych w świetle Karty praw podstawowych Unii Europejskiej;
   - dopilnować, by ustanowienie w ramach Europolu unijnej jednostki ds. zgłaszania podejrzanych treści w internecie (EU IRU) opierało się na odpowiedniej z punktu widzenia działalności tej jednostki podstawie prawnej;
   - zapewnić specjalne środki służące zwalczaniu wykorzystywania seksualnego dzieci w internecie oraz skuteczną współpracę między wszystkimi zainteresowanymi stronami w celu zagwarantowania praw i ochrony dzieciom korzystającym z internetu oraz sprzyjania inicjatywom, które dążą do tego, by internet stał się bezpieczny dla dzieci

– oraz współpracować z odnośnymi zainteresowanymi stronami na rzecz promowania kampanii edukacyjnych i podnoszących świadomość;

3. przypomina, że zgodnie z art. 12 dyrektywy o handlu elektronicznym (2000/31/WE) „państwa członkowskie zapewniają, żeby w przypadku świadczenia usługi społeczeństwa informacyjnego polegającej na transmisji w sieci telekomunikacyjnej informacji przekazanych przez usługobiorcę lub na zapewnianiu dostępu do sieci telekomunikacyjnej usługodawca nie był odpowiedzialny za przekazywane informacje, jeżeli: a) nie jest inicjatorem przekazu; b) nie wybiera odbiorcy przekazu; oraz c) nie wybiera oraz nie modyfikuje informacji zawartych w przekazie”;

3.4. Wzmocnienie zaufania do usług cyfrowych i przetwarzania danych osobowych oraz zwiększenie bezpieczeństwa takich usług i danych

4. zwraca uwagę na fakt, że szybko rosnąca liczba ataków na sieci oraz aktów cyberprzestępczości wymaga zharmonizowanej reakcji UE i jej państw członkowskich w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji; uważa, że zapewnienie bezpieczeństwa w internecie wymaga ochrony sieci i infrastruktury krytycznej, zagwarantowania zdolności organów ścigania do zwalczania przestępczości, w tym terroryzmu, brutalnej radykalizacji, niegodziwego traktowania w celach seksualnych i wykorzystywania seksualnego dzieci w internecie, a także wykorzystywania danych, które są absolutnie niezbędne do zwalczania przestępczości online i offline; podkreśla, że zdefiniowane w ten sposób bezpieczeństwo oraz ochrona praw podstawowych w cyberprzestrzeni są niezbędne, aby wzmocnić zaufanie do usług cyfrowych, a także że stanowią one zatem konieczną podstawę do utworzenia konkurencyjnego jednolitego rynku cyfrowego;

5. apeluje o ostateczne przyjęcie dyrektywy o bezpieczeństwie sieci i informacji w celu uchwalenia spójnych ram regulacyjnych dla zapewnienia strategicznego i operacyjnego cyberbezpieczeństwa na szczeblu unijnym i krajowym, które wymaga ściślejszej współpracy z władzami krajowymi i agencjami UE, przy jednoczesnym zapewnieniu ochrony praw podstawowych UE, zwłaszcza prywatności i ochrony danych przedsiębiorstw, administracji publicznej i podmiotów danych;

6. przypomina, że metody takie jak szyfrowanie są użyteczne dla obywateli i przedsiębiorstw, ponieważ umożliwiają zapewnienie prywatności oraz co najmniej podstawowego poziomu bezpieczeństwa łączności; potępia fakt, że metody te mogą być również stosowane do celów przestępczych;

7. z zadowoleniem przyjmuje ustanowienie w ramach Europolu Europejskiego Centrum ds. Walki z Cyberprzestępczością (EC3), które przyczynia się do szybszej odpowiedzi na cyberataki; domaga się wniosku ustawodawczego przewidującego wzmocnienie mandatu EC3 oraz apeluje o szybką transpozycję dyrektywy 2013/40/UE z dnia 12 sierpnia 2013 r. dotyczącej ataków na systemy informatyczne, której celem jest także poprawa współpracy operacyjnej między organami ścigania państw członkowskich i właściwymi agencjami UE (Eurojust, Europol, EC3 i Agencja Unii Europejskiej ds. Bezpieczeństwa Sieci i Informacji (ENISA));

8. z zadowoleniem przyjmuje inicjatywę Komisji na rzecz ustanowienia partnerstwa publiczno-prywatnego w sprawie cyberbezpieczeństwa; zwraca uwagę na potrzebę

współpracy i zaangażowania przedsiębiorstw oraz wprowadzenia koncepcji uwzględniania bezpieczeństwa na etapie projektowania; popiera wymianę przez państwa członkowskie dobrych praktyk dotyczących partnerstw publiczno-prywatnych w tej dziedzinie; ubolewa w związku z tym nad zamknięciem europejskiego partnerstwa publiczno-prywatnego na rzecz odporności (EP3R);

9. zauważa, że doniesienia o masowej elektronicznej inwigilacji świadczą o potrzebie odzyskania zaufania obywateli do prywatności, bezpieczeństwa i ochrony usług cyfrowych; podkreśla w związku z tym, że przy przetwarzaniu danych osobowych do celów komercyjnych lub do celów egzekwowania prawa należy ściśle przestrzegać obowiązujących przepisów o ochronie danych i praw podstawowych; przypomina w związku z tym o znaczeniu istniejących narzędzi takich jak umowy o wzajemnej pomocy prawnej, w ramach których przestrzega się praworządności i ogranicza ryzyko niedozwolonego dostępu do danych, które są przechowywane na obcym terytorium;

10. podkreśla, że zgodnie z art. 15 ust. 1 dyrektywy 2000/31/WE w sprawie handlu elektronicznego państwa członkowskie nie nakładają na usługodawców świadczących usługi transmisji, przechowywania i hostingu ogólnego obowiązku nadzorowania informacji, które przekazują lub przechowują, ani ogólnego obowiązku aktywnego poszukiwania faktów i okoliczności wskazujących na bezprawną działalność; przypomina w szczególności, że Trybunał Sprawiedliwości Unii Europejskiej w wyrokach C-360/10 i C-70/10 odrzucił środki „aktywnego nadzoru" nad prawie wszystkimi odnośnymi usługobiorcami (w jednym wyroku chodziło o dostawców usług internetowych, a w drugim o sieć społecznościową) i sprecyzował, że wszelkie narzucanie podmiotom świadczącym usługi hostingu obowiązku prowadzenia ogólnego nadzoru powinno być zakazane;

4.1. Budowanie gospodarki opartej na danych

11. jest zdania, że duże zbiory danych, chmury obliczeniowe, internet przedmiotów, badania naukowe i innowacje są kluczowymi czynnikami rozwoju gospodarczego i wymagają spójnego podejścia w całym prawodawstwie UE; uważa, że przestrzeganie przepisów o ochronie danych i skuteczne gwarancje prywatności i bezpieczeństwa ustanowione w ogólnym rozporządzeniu o ochronie danych, w tym szczegółowe przepisy dotyczące dzieci jako konsumentów podatnych na zagrożenia, mają zasadnicze znaczenie dla budowania zaufania obywateli i konsumentów do sektora gospodarki opartej na danych; zwraca uwagę na konieczność podnoszenia świadomości na temat roli danych i znaczenia wymiany danych dla konsumentów, w odniesieniu do ich praw podstawowych oraz w gospodarce, a także ustanowienia przepisów w dziedzinie własności danych i sprawowania przez obywateli kontroli nad swoimi danymi osobowymi; zwraca uwagę na rolę personalizacji usług i produktów, którą należy rozwijać zgodnie z wymogami ochrony danych; apeluje o propagowanie uwzględniania ochrony prywatności już w fazie projektowania i domyślnej ochrony prywatności, co może również pozytywnie wpłynąć na innowacje i wzrost gospodarczy; podkreśla potrzebę zapewnienia niedyskryminacyjnego podejścia do wszelkich operacji przetwarzania danych; zwraca uwagę na znaczenie podejścia opartego na analizie ryzyka, które pomaga uniknąć zbędnych obciążeń administracyjnych i zapewnia pewność prawa, tak jak w ogólnym rozporządzeniu o ochronie danych, zwłaszcza MŚP i przedsiębiorstwom typu start-up, a także na znaczenie nadzoru demokratycznego i stałego monitorowania przez władze

publiczne; podkreśla, że dane osobowe wymagają specjalnej ochrony i uznaje, że ustanowienie dodatkowych gwarancji, takich jak pseudonimizacja lub anonimizacja, może zwiększyć ochronę, w przypadku gdy dane osobowe są wykorzystywane w aplikacjach dużych zbiorów danych i przez dostawców usług internetowych;

4.2. Zwiększenie konkurencyjności dzięki interoperacyjności i normalizacji

12. podkreśla, że przetwarzanie danych osobowych za pomocą rozwiązań opartych na interoperacyjności, tj. realizowanych dzięki programowi ISA², musi być zgodne z wymogami unijnych przepisów w dziedzinie ochrony danych; apeluje o lepszą współpracę, aby ustanowić wspólne globalne standardy gospodarki opartej na danych, które to standardy powinny wysuwać na pierwszy plan bezpieczeństwo, poszanowanie prywatności i ochronę danych; podkreśla znaczenie prawa obywateli do do przenoszenia danych;

4.3.2. E-administracja

13. popiera cyfryzację usług publicznych w Europie, rozwój e-administracji, e-demokracji i polityki otwartego dostępu do danych, dostęp do dokumentów sektora publicznego i ich ponowne wykorzystywanie w oparciu o zasadę przejrzystości i istniejące ramy prawne UE oraz wysokie standardy ochrony danych, zaproponowane w pakiecie reform w dziedzinie ochrony danych, przy pełnym poszanowaniu Karty praw podstawowych; przypomina, że e-administracja przyczynia się do rzeczywistego udziału, konsultacji oraz przejrzystszej, bardziej odpowiedzialnej i skutecznej administracji publicznej; podkreśla w związku z tym znaczenie wymiany najlepszych praktyk między wszystkimi zainteresowanymi podmiotami;

14. popiera rozwój e-administracji, w tym propagowanie zasady jednorazowości, podkreślając jednocześnie, że wszystkie inicjatywy dotyczące e-administracji muszą spełniać wymogi i być zgodne z zasadami pakietu reform w dziedzinie ochrony danych oraz że należy zapewnić wysoki poziom bezpieczeństwa tych inicjatyw, aby chronić dane obywateli udostępniane instytucjom publicznym;

5.2. Wymiar międzynarodowy

15. uznaje globalny charakter gospodarki opartej na danych; przypomina, że utworzenie jednolitego rynku cyfrowego zależy od swobodnego przepływu danych w Unii Europejskiej i poza nią; apeluje zatem, by UE i jej państwa członkowskie we współpracy z państwami trzecimi podjęły działania w celu dopilnowania, by współpraca z państwami trzecimi w ramach Strategii jednolitego rynku cyfrowego dla Europy charakteryzowała się wysokimi standardami ochrony danych i bezpieczeństwem międzynarodowego przesyłania danych, zgodnie z ogólnym rozporządzeniem o ochronie danych i orzecznictwem UE.

WYNIK GŁOSOWANIA KOŃCOWEGO W KOMISJI OPINIODAWCZEJ

Data przyjęcia	30.11.2015
Wynik głosowania końcowego	+: 49 –: 1 0: 2
Posłowie obecni podczas głosowania końcowego	Jan Philipp Albrecht, Michał Boni, Ignazio Corrao, Agustín Díaz de Mera García Consuegra, Frank Engel, Kinga Gál, Ana Gomes, Nathalie Griesbeck, Sylvie Guillaume, Jussi Halla-aho, Monika Hohlmeier, Brice Hortefeux, Sophia in ‘t Veld, Sylvia-Yvonne Kaufmann, Barbara Kudrycka, Marju Lauristin, Juan Fernando López Aguilar, Roberta Metsola, Louis Michel, Claude Moraes, Alessandra Mussolini, József Nagy, Soraya Post, Judith Sargentini, Birgit Sippel, Branislav Škripek, Csaba Sógor, Helga Stevens, Bodil Valero, Marie-Christine Vergiat, Harald Vilimsky, Udo Voigt, Beatrix von Storch, Josef Weidenholzer, Cecilia Wikström, Kristina Winberg, Tomáš Zdechovský
Zastępcy obecni podczas głosowania końcowego	Carlos Coelho, Anna Hedh, Teresa Jiménez-Becerril Barrio, Marek Jurek, Ska Keller, Miltiadis Kyrkos, Jeroen Lenaers, Nuno Melo, Emilian Pavel, Morten Helveg Petersen, Barbara Spinelli, Axel Voss
Zastępcy (art. 200 ust. 2) obecni podczas głosowania końcowego	Jens Geier, Gabriele Preuß, Marco Zanni