



PARLAMENT EUROPEJSKI

2009 - 2014

Komisja Rynku Wewnętrznego i Ochrony Konsumentów

2011/2025(INI)

14.4.2011

OPINIA

Komisji Rynku Wewnętrznego i Ochrony Konsumentów

dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych

w sprawie całościowego podejścia do kwestii ochrony danych osobowych
w Unii Europejskiej
(2011/2025(INI))

Sprawozdawca: Projekt opinii

PA_NonLeg

WSKAZÓWKI

Komisja Rynku Wewnętrznego i Ochrony Konsumentów zwraca się do Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, właściwej dla tej sprawy, o uwzględnienie w końcowym tekście projektu rezolucji następujących wskazówek:

- A. mając na uwadze, że dyrektywa w sprawie ochrony danych 95/46/WE i dyrektywa pakietu telekomunikacyjnego UE 2009/140/WE umożliwiają swobodny przepływ danych osobowych na rynku wewnętrznym;
- B. mając na uwadze, że w internecie powstaje coraz więcej różnego rodzaju sieci społecznych i że przede wszystkim młodzi ludzie ujawniają przy tym swoje dane osobowe;
- C. mając na uwadze, że podstawowe założenia dyrektywy 1995/46/WE są nadal aktualne, globalizacja i szybki rozwój technologiczny przyniosły nowe wyzwania w zakresie ochrony danych osobowych w wyniku zwiększonego uzależnienia od kompleksowych informatycznych narzędzi technologicznych stosowanych do przetwarzania danych oraz zwiększonej działalności w internecie, w tym również handlu elektronicznego, e-zdrowia, elektronicznej administracji, rosnącej popularności sieci społecznościowych, rozwoju internetowych reklam behawioralnych lub obliczania rozproszonego (ang. cloud computing);
- D. mając na uwadze, że rosnąca wymiana indywidualnych danych osobowych w połączeniu z nowymi wynalazkami technologicznymi doprowadziły do zwiększonego gromadzenia, magazynowania i korzystania z danych osobowych, i spowodowały pojawienie się problemu z określeniem prawa właściwego i zdefiniowaniem obowiązków wszystkich zainteresowanych stron, jeśli chodzi o stosowanie unijnego ustawodawstwa w zakresie ochrony danych (np. firma w posiadaniu danych osobowych obywateli UE, której siedziba znajduje się poza UE i która zleca wykonawstwo firmom, które także mają siedzibę poza UE);
- E. mając na uwadze, że zmiana dyrektywy o ochronie danych 95/46/WE powinna polegać na kompleksowej reformie unijnych ram prawnych dotyczących ochrony danych, określając surowsze przepisy dotyczące gromadzenia danych, zwłaszcza jeśli chodzi o informowanie danej osoby o tym dlaczego, kto i jak długo gromadzi i wykorzystuje jej dane, i to zarówno w internecie, jak i poza nim;
- F. mając na uwadze, że obywatele nie dokonują zakupów w internecie tak samo bezpiecznie jak poza nim, z powodu obaw o kradzież tożsamości i braku przejrzystości co do sposobu w jaki ich dane osobowe są przetwarzane i wykorzystywane;
- G. mając na uwadze, że przedsiębiorstwa i sektor handlowy coraz częściej wykorzystują karty stałego klienta (np. karty do klubów, karty rabatowe lub lojalnościowe), które służą lub mogą służyć do tworzenia profili klientów;
- H. mając na uwadze, że dane gromadzone za pośrednictwem kart stałego klienta są wykorzystywane do tworzenia profili klientów, a ponadto mając na uwadze, że powstał

rynek, na którym handluje się takimi danymi;

1. wzywa do wzmocnienia wymiaru ochrony danych na rynku wewnętrznym w internecie i poza nim poprzez pełne ujednoczenie ustawodawstw państw członkowskich, po gruntownej ocenie skutków i analogicznie do ram prawnych dotyczących telekomunikacji, zgodnie z najwyższymi standardami ochrony danych w celu zwiększenia pewności prawnej, zapewnienia spójnego poziomu ochrony prywatności, zredukowania obciążenia administracyjnego i kosztów, zapobiegania ryzyku wyboru sądu ze względu na możliwość korzystniejszego wyroku pomiędzy bardziej lub mniej surowymi ustawodawstwami krajowymi państw członkowskich i zagwarantowania równych szans wszystkim podmiotom gospodarczym i administratorom danych; uważa, że będzie to stymulować wspólny rynek cyfrowy i zredukuje nadmierne koszty ponoszone przez przedsiębiorstwa, zwłaszcza przez MŚP;
2. uważa, że wdrożenie unijnych przepisów dotyczących ochrony danych w UE jest nadal nierównomierne i fragmentaryczne, co ma negatywny wpływ na podstawowe prawa i swobody obywateli w zakresie ochrony danych i prywatności, pewności prawnej i przejrzystości w stosunkach umownych, rozwoju handlu elektronicznego i e-biznesu, zaufania konsumentów do systemu, transakcji ponadgranicznych i zapewnienia prawdziwie równych szans przedsiębiorstwom i MŚP w ramach wspólnego rynku;
3. stwierdza, że ochrona danych na rynku wewnętrznym musi odgrywać coraz większą rolę;
4. domaga się szybkiego opracowania na nowo istniejących ram prawnych UE dotyczących ochrony danych, szczególnie w kontekście rosnącego zagrożenia, jakie dla praw indywidualnych stanowią nowe formy przetwarzania danych, jak choćby tworzenie profili lub niepożądany transfer danych;
5. apeluje zwłaszcza o dostosowanie przepisów o ochronie danych do podstawowych zasad zawartych w dyrektywie o prywatności i łączności elektronicznej we wszystkich obszarach ochrony danych w celu unikania rozwiązań cząstkowych;
6. podkreśla zapotrzebowanie na funkcjonujący wspólny rynek odnośnie do spójnego, całościowego i skutecznego egzekwowania przepisów o ochronie danych, biorąc pod uwagę wpływ nowych technologii na prawa osób fizycznych, przejrzystość procedur i uzasadnione interesy zainteresowanych osób, przy jednoczesnym zagwarantowaniu możliwości przenoszenia danych osobowych w celu ułatwienia sprawnego funkcjonowania zarówno rynku wewnętrznego, jak i internetu i jego charakterystycznej otwartości i interoperacyjności;
7. jest zdania, że wszelkie dane osobowe i informacje przekazywane pomiędzy różnymi wspólnymi punktami kontaktowymi i w ramach systemu wymiany informacji na rynku wewnętrznym (IMI) są przetwarzane, wykorzystywane i gromadzone tylko w zgodnych z prawem celach oraz że stosowane są niezbędne zabezpieczenia przed nadużyciami;
8. zwraca uwagę na znaczenie aktualizacji dyrektywy w miarę światowego postępu technologicznego;
9. uważa, że zasadniczo tworzenie profili powinno być dopuszczalne jedynie w oparciu

o konkretne podstawy prawne lub o świadomą zgodę zainteresowanych osób, która powinna być dobrowolna i z której można się w każdej chwili wycofać;

10. zauważa, że rozwój i szersze stosowanie obliczania rozproszonego (ang. cloud computing) stawia przed nami nowe wyzwania w zakresie prywatności i ochrony danych osobowych; w związku z tym apeluje o jasne przedstawienie możliwości administratorów danych i przetwarzających dane oraz hostów, aby lepiej podzielić między nich spoczywające na nich zobowiązania prawne oraz aby osoby, których dotyczą dane, wiedziały gdzie są one przechowywane, kto ma do nich dostęp, kto decyduje o sposobie ich wykorzystania oraz o istniejących systemach tworzenia zapasowych kopii danych i ich odzyskiwania;
11. zwraca uwagę na konieczność działań edukacyjnych i służących pogłębieniu świadomości oraz ukierunkowanych strategii komunikacyjnych w zakresie ochrony danych dla usługodawców, jak również obywateli i konsumentów; wzywa do podjęcia pilnych środków służących zapewnieniu, że obywatele będą odpowiednio poinformowani o swych prawach i obowiązkach, jeśli chodzi o wykorzystywanie ich danych osobowych, krótko- i długofalowe konsekwencje udostępniania pewnego typu danych, różne modele wyrażania zgody, możliwość przenoszenia danych, ochronę ich prywatności oraz instrumenty, którymi dysponują, aby zapobiegać sytuacjom zagrażającym ich prawu do prywatności, takie jak tzw. prawo do bycia zapomnianym (a mianowicie prawo osób fizycznych do spowodowania zaprzestania dalszego gromadzenia, analizowania, przetwarzania czy wykorzystywania ich danych osobowych w jakikolwiek sposób oraz ich usunięcia, jeżeli przestały być potrzebne do przewidzianych prawem celów), w szczególności w środowisku internetowym;
12. wzywa Komisję do wzmocnienia, wyjaśnienia i ujednolicenia przepisów dotyczących dobrowolnej i świadomej zgody oraz do sprecyzowania warunków umów; domaga się, aby zasadniczo każda osoba musiała udzielić wcześniejszej zgody, zanim jej dane będzie można zebrać, ocenić, zapisać w formie profilu lub przekazać dalej; domaga się również, aby takie dane musiały być ujawniane na żądanie zainteresowanej osoby, a także usuwane najpóźniej z chwilą, gdy osoba ta o to wystąpi; podkreśla konieczność jasnego komunikowania osobom, których dotyczą dane, poziomu adekwatności ochrony danych w krajach trzecich;
13. zwraca uwagę, że kwestie ochrony danych dotyczą zarówno konsumentów i przedsiębiorstw jak i pracowników; domaga się zatem uwzględnienia wysokich standardów ochrony danych pracowników, aby ograniczać niestosowną kontrolę danych osobowych personelu;
14. wzywa Komisję do wyjaśnienia przepisów dotyczących prawa właściwego w dziedzinie ochrony danych osobowych, gdyż coraz trudniejsze staje się określenie obowiązków zainteresowanych stron z powodu globalizacji wymiany; podkreśla, że konieczne jest zagwarantowanie pewności prawnej administratorom danych i unikanie luk w ochronie danych osobowych, którą zapewnia dyrektywa 95/46/WE;
15. podkreśla, że osoby zainteresowane powinny mieć zawsze możliwość wpływu na dotyczące ich działania gospodarcze; ponadto osoby zainteresowane muszą mieć zawsze możliwość korzystania z przysługującego im prawa do podejmowania niezależnych

decyzji w oparciu o przekazane im dostateczne informacje;

16. zwraca uwagę Komisji na wysoce strategiczny charakter lokalizacji centrów danych i na potencjalne konsekwencje umieszczenia takiej lokalizacji poza terytorium UE;
17. z zadowoleniem przyjmuje propozycje Komisji w sprawie systemu obowiązkowego zawiadamiania o naruszeniu ochrony danych osobowych w dyrektywie o prywatności i łączności elektronicznej, które powinny ponadto być stosowane w sposób spójny we wszystkich obszarach, w których wymagana jest ochrona danych; domaga się przeglądu i uproszczenia obowiązującego systemu obowiązkowego zawiadamiania o przetwarzaniu danych osobowych poza sektor telekomunikacji z uwzględnieniem poważnych przypadków łamania przepisów dotyczących ochrony, aby zagwarantować, że wymogi dotyczące przetwarzania danych nie obciążą nadmiernie administratorów danych i położyć kres zróżnicowaniu krajowych wymogów w tej dziedzinie; domaga się rozszerzenia systemu obowiązkowego zawiadamiania o naruszeniu ochrony danych osobowych poza sektor telekomunikacji na poważne przypadki łamania przepisów dotyczących ochrony danych, podkreślając znaczenie jednolitego systemu powiadamiania o naruszeniach;
18. podkreśla, że prawo osób do podejmowania niezależnych decyzji musi być traktowane priorytetowo i że każda osoba ma prawo otrzymać bezpłatnie informacje dotyczące zgromadzonych na jej temat danych oraz prawo do ich usunięcia, zwłaszcza profili, stworzonych w celach komercyjnych;
19. podkreśla znaczenie, jakie dla przechowujących dane osobowe ma wyznaczenie jednego administratora odpowiedzialnego za ochronę danych o jasno określonych zadaniach; uważa, że podmioty działające na wspólnym rynku powinny móc wyznaczyć administratora odpowiedzialnego za ochronę danych dla ich działań w UE;
20. wzywa Komisję, aby podczas przeglądu dyrektywy 95/46/WE należycie uwzględniła kwestie ochrony prywatności dotyczące obliczania rozproszonego oraz zapewniła, że przepisy dotyczące ochrony danych będą miały zastosowanie do wszystkich interesariuszy, w tym operatorów sieci telekomunikacji i nie tylko, gwarantując jednocześnie rozwój obliczania rozproszonego;
21. podkreśla, że procedury dotyczące dostępu do danych osobowych muszą być wyraźnie i natychmiast dostępne obywatelom we wszystkich państwach członkowskich, wspomagane siecią punktów kontaktowych i udostępniane w internecie; apeluje zwłaszcza o uproszczenie przepisów wykonawczych;
22. wzywa Komisję do zbadania możliwości dostępu, poprawiania i usuwania danych, a także korzystania z alternatywnych metod rozwiązywania sporów na rynku wewnętrznym, w szczególności w środowisku internetowym, oraz podkreśla, że konieczna jest odpowiednia polityka ścigania naruszeń;
23. zachęca do rozszerzenia zdolności władz krajowych do egzekwowania prawa, w tym wobec przedsiębiorstw spoza UE, których działalność jest ukierunkowana na konsumentów w UE;

24. podkreśla konieczność propagowania wykorzystania technologii podnoszących poziom ochrony prywatności i stosowania zasady uwzględniania ochrony prywatności w fazie projektowania, aby zagwarantować, że kwestie związane z ochroną prywatności zostaną uwzględnione podczas przyszłych faz rozwoju technologicznego; wzywa Komisję do zachęcenia dostawców technologii do włączenia podstawowych zasad ochrony prywatności, w tym minimalizacji danych, przejrzystości i kontroli użytkowników podczas rozwoju i wdrażania technologii w celu zagwarantowania wysokiego poziomu ochrony danych osobowych na całym wspólnym rynku;
25. wzywa Komisję do zbadania, we współpracy z CEN, możliwości opracowania standardów obsługi w zakresie zarządzania danymi osobowymi i rozwoju powiązanych narzędzi zarządzania informacją, z należyтым uwzględnieniem ochrony prywatności w fazie projektowania; uważa, że takie standardy projektowe będą propagować najlepsze praktyki w rozwoju systemów zarządzania danymi, a w szczególności zwiększą bezpieczeństwo zarządzania bazami danych i aplikacji służących przechowywaniu; podkreśla jednak, że wszystkie wnioski powinny być neutralne pod względem technologicznym i przyjazne innowacjom;
26. wzywa Komisję do przeglądu wraz z CEN europejskich norm dotyczących przechowywania sprzętu z należyтым uwzględnieniem ochrony prywatności w fazie projektowania i do zachęcania do rozwoju norm produkcji umożliwiających ostateczne usunięcie danych przechowywanych na sprzęcie, który nie jest już używany do przechowywania danych osobowych lub tak czy inaczej wychodzi z użytku; uważa ponadto, że takie standardy projektowe będą propagować najlepsze praktyki produkcyjne; podkreśla jednak, że wszystkie wnioski powinny być neutralne pod względem technologicznym i przyjazne innowacjom;
27. apeluje o zwiększenie roli Grupy Roboczej art. 29 i sformalizowanie jej roli w procesie wdrażania standardowych zasad ochrony danych i utrzymania jej niezależności od Komisji Europejskiej;
28. zwraca się do Komisji, aby przeprowadziła ocenę wpływu inicjatyw samoregulacyjnych jako narzędzi umożliwiających lepsze egzekwowanie przepisów o ochronie danych.
29. zachęca do rozwoju unijnego systemu certyfikacji w obszarze prywatności i ochrony danych. Powinien on być skonstruowany w taki sposób, aby unikać nadmiernego obciążania przedsiębiorstw – a zwłaszcza MŚP – kosztownymi i biurokratycznymi obowiązkami, które mogą zniechęcać do udziału w nim. System powinien być neutralny pod względem technologicznym, gotowy do stosowania na całym świecie i przystępny cenowo, aby nie tworzyć barier blokujących udział.
30. popiera utworzenie unijnego systemu certyfikacji dla stron internetowych zgodnego z ustawodawstwem UE w zakresie ochrony danych i wzorowanego na europejskiej marce ochrony danych osobowych (dobrowolna ogólnoeuropejska etykieta poświadczająca przestrzeganie przez produkty i usługi IT unijnego ustawodawstwa z zakresu ochrony danych), który miałby zastosowanie w całej UE i zastąpiłby różne istniejące prywatne systemy certyfikacji i oznakowania, które często są uznawane tylko na skalę lokalną; uważa, że przed jego przyjęciem należy przeprowadzić gruntowną ocenę skutków;

31. uważa, że rozwój i propagowanie inicjatyw samoregulacyjnych może poprawić stan obowiązujących ram ochrony danych, choć nie mogą one zastąpić środków ustawodawczych, zwłaszcza jeśli chodzi o ich egzekwowanie; zwraca się do Komisji i państw członkowskich, aby sprzyjały takim inicjatywom oraz opracowywały i wspierały instrumenty, dzięki którym samoregulacja staje się atrakcyjniejsza dla gospodarki;
32. wzywa Komisję, by zbyt daleko posunięta harmonizacja nie ograniczała sprawdzonych systemów ochrony danych, takich jak wewnętrzne kontrole ochrony danych w przedsiębiorstwach przeprowadzane przez zakładowych inspektorów ochrony danych oraz kontrole zewnętrzne dokonywane przez państwowe organy nadzoru ochrony danych;
33. popiera utworzenie wspólnych i jasnych kryteriów na szczeblu UE w celu przeprowadzenia kontroli w dziedzinie ochrony prywatności i danych.
34. z zadowoleniem przyjmuje stanowisko Komisji w sprawie wzajemności w poziomie ochrony danych osób, których dane są eksportowane do krajów trzecich lub w nich przechowywane; wzywa jednak Komisję do podjęcia decydujących kroków w kierunku zacieśnienia współpracy regulacyjnej z krajami trzecimi z myślą o wyjaśnieniu prawa właściwego i konwergencji ustawodawstwa UE i krajów trzecich w zakresie ochrony danych; wzywa Komisję do priorytetowego potraktowania tego zagadnienia w ramach ponownie wznowionej Transatlantyckiej Rady Gospodarczej;
35. wzywa do rozwoju łatwiejszych, wydajniejszych metod pozwalających na międzynarodowy transfer danych, przy zachowaniu odpowiednich poziomów ochrony danych i prywatności osób;
36. wzywa Komisję do podtrzymania obowiązujących wyłączeń i odstępstw zawartych w art. 9 dyrektywy 95/46/WE od pewnych przepisów dotyczących ochrony danych w celach dziennikarskich, aby chronić wolne i niezależne media w UE lub w celu uzyskania wyrazu artystycznego lub literackiego, aby wspierać twórczość.

WYNIK GŁOSOWANIA KOŃCOWEGO W KOMISJI

Data przyjęcia	13.4.2011
Wynik głosowania końcowego	+: 36 -: 0 0: 0
Posłowie obecni podczas głosowania końcowego	Pablo Arias Echeverría, Adam Bielan, Lara Comi, Anna Maria Corazza Bildt, António Fernando Correia De Campos, Jürgen Creutzmann, Christian Engström, Evelyne Gebhardt, Louis Grech, Małgorzata Handzlik, Iliana Ivanova, Philippe Juvin, Sandra Kalniete, Eija-Riitta Korhola, Edvard Kožušník, Kurt Lechner, Toine Manders, Mitro Repo, Robert Rochefort, Zuzana Roithová, Heide Rühle, Matteo Salvini, Christel Schaldemose, Andreas Schwab, Eva-Britt Svensson, Róza Gräfin von Thun und Hohenstein, Kyriacos Triantaphyllides, Emilie Turunen, Bernadette Vergnaud, Barbara Weiler
Zastępca(y) obecny(i) podczas głosowania końcowego	Ashley Fox, María Irigoyen Pérez, Pier Antonio Panzeri, Konstantinos Poupakis, Sylvana Rapti, Olle Schmidt