

Środa, 14 lutego 2007 r.

39. zachęca do znacznie większego bezpośredniego zaangażowania w wysiłki mające na celu łagodzenie zmian klimatu, dokonywane na poziomie obywateli europejskich; wzywa zatem Komisję do zintensyfikowania działań podnoszących świadomość o tym, jak nagła jest sytuacja w tym zakresie, w celu informowania obywateli o ich roli w kontrolowaniu zmian klimatu;
40. wzywa ponownie Unię Europejską i państwa członkowskie do przyjęcia ambitnej polityki partnerstwa technologicznego i transferu czystych technologii z krajami rozwijającymi się w celu wsparcia ich w rozwoju gospodarki i zwiększeniu dobrobytu w bardziej trwały sposób;
41. wzywa Komisję Europejską do dokonania oceny wpływu zmian klimatycznych na wzrost temperatury ziemi, zmniejszenie ilości opadów oraz stan podziemnych zasobów wodnych; uważa za szczególnie ważne badanie skutków ograniczenia powierzchni uprawnych jako źródła biomasy i złóż węgla; podkreśla znaczenie niektórych praktyk zarządzania rolnego;
42. wzywa wszystkie odpowiednie komisje i delegacje do ścisłej współpracy w zakresie zmian klimatycznych, tak aby lepiej skoordynować politykę przemysłową, politykę energetyczną transport, rolnictwo, badania i rozwój oraz inne inicjatywy z celami związanymi ze zmianami klimatycznymi i tak aby kwestię spraw klimatycznych regularnie poruszać na szczelbu delegacji międzyparlamentarnych oraz w kontekście transatlantyckiego dialogu legislacyjnego;
43. wzywa trzy prezydencje (Niemcy, Portugalię i Słowenię) do zapewnienia, że kwestia zmian klimatycznych nabierze rozmachu, a poziom zobowiązań politycznych oraz liczba partnerów międzynarodowych w procesie na szczelbu międzynarodowym wzrośnie;
44. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, rządowi i parlamentom państw członkowskich oraz sekretariatowi UNFCCC z prośbą o przekazanie wszystkim krajom-stronom tej konwencji nienależącym do UE.

P6_TA(2007)0039

PNR-SWIFT

Rezolucja Parlamentu Europejskiego w sprawie SWIFT, porozumienia dotyczącego PNR oraz dialogu transatlantyckiego w tych kwestiach

Parlament Europejski,

- uwzględniając oświadczenia Rady i Komisji w trakcie debaty, która miała miejsce w Parlamencie w dniu 31 stycznia 2007 r. w następstwie pytania ustnego na temat firmy SWIFT oraz negocjacji w sprawie nowego porozumienia UE-USA dotyczącego przekazywania danych dotyczących pasażerów (PNR),
- uwzględniając pisemną odpowiedź Europejskiego Banku Centralnego z dnia 30 stycznia 2007 r. na skierowane doń pytanie podnoszące kwestię, że EBC nie poinformował właściwych organów ochrony danych oraz banków centralnych (skreślenie) o stosowanej przez Stany Zjednoczone praktyce dostępu do danych dotyczących transakcji finansowych generowanych przez SWIFT, oraz nie zastosował leżącej w jego mocy moralnej perswazji w stosunku do SWIFT,
- uwzględniając opinię grupy roboczej w sprawie ochrony osób fizycznych w odniesieniu do przetwarzania danych osobowych, zgodnie z art. 29 dyrektywy o ochronie danych⁽¹⁾ (grupa robocza ds. art. 29) w sprawie przyszłego porozumienia dotyczącego PNR, a także opinię Europejskiego Inspektora Danych Osobowych (EDPS) na temat roli EBC w sprawie SWIFT,
- uwzględniając art. 103 ust. 2 Regulaminu,

⁽¹⁾ Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych (Dz.U. L 281 z 23.11.1995, str. 31).

Środa, 14 lutego 2007 r.

- A. mając na uwadze, że udostępnianie danych i informacji stanowi cenne narzędzie międzynarodowej walki z terroryzmem i przestępczością z nim związaną,
- B. mając na uwadze, że podmioty gospodarcze prowadzące działalność po obu stronach Atlantyku coraz częściej wpadają w pułapkę sprzecznych wymogów prawnych jurysdykcji amerykańskiej i europejskiej,
- C. mając na uwadze, że udostępnianie danych osobowych musi się opierać na właściwej podstawie prawnej, podlegać jasnym zasadom i warunkom oraz musi mu towarzyszyć odpowiednia ochrona prywatności i swobód obywatelskich poszczególnych obywateli,
- D. mając na uwadze, że walka z terroryzmem i przestępczością musi mieć właściwą legitymację demokratyczną, co oznacza, że programy udostępniania danych muszą podlegać nieustannej kontroli parlamentarnej i sądowej;

Kwestie ogólne

1. podkreśla, że w ciągu kilku ostatnich lat kilka porozumień wynikających z wymogów amerykańskich i przyjętych bez jakiegokolwiek udziału Parlamentu Europejskiego – zwłaszcza porozumienie w sprawie PNR i protokół SWIFT – a także istnienie amerykańskiego systemu automatycznego naprowadzania (ATS) doprowadziło do sytuacji niepewności prawnej w odniesieniu do niezbędnych gwarancji ochrony danych dotyczących udostępniania i przekazywania danych między UE i USA w celach zapewnienia bezpieczeństwa publicznego, a w szczególności zapobiegania terroryzmowi i zwalczania go;
2. ponownie stwierdza, że rozwiązania rozważane do tej pory przez Radę i Komisję, a także przez prywatne przedsiębiorstwa, nie zapewniają odpowiedniej ochrony danych osobowych obywateli UE (co odnotowano również w piśmie P. Schaara, przewodniczącego grupy roboczej ds. art. 29, w sprawie nowego porozumienia przejściowego dotyczącego PNR) oraz że może to stanowić pogwałcenie prawa wspólnotowego i krajowego, jak w przypadku SWIFT (patrz opinia 10/2006 grupy roboczej ds. art. 29 z dnia 22 listopada 2006 r. oraz opinia Europejskiego Inspektora Danych Osobowych z dnia 1 lutego 2007 r.);
3. zauważa, że w ramach walki z terroryzmem Kongres USA przez pewien czas zwracał się do administracji USA o przyjęcie bardziej ukierunkowanych działań na rzecz lepszej ochrony prywatności, podlegających kontroli parlamentarnej i sądowej (o co zwrócono się, gdy Kongres został poinformowany o istnieniu programu Agencji Bezpieczeństwa Narodowego (ABN) dotyczącego podsłuchu telefonicznego);
4. potwierdza zastrzeżenia, z którymi ostatnio zgodził się Kongres, dotyczące metody profilowania i eksploracji danych polegającej na niewybiórczym gromadzeniu coraz większej ilości danych osobowych, tak jak w przypadku systemu ATS stosowanego przez administrację USA;
5. z zadowoleniem przyjmuje fakt, że w ostatnim czasie administracja USA przyjęła powyższe zastrzeżenia do wiadomości i będzie się starać o poprawę sytuacji za pomocą następujących działań:
 - a) powołania urzędników ds. ochrony prywatności i/lub niezależnej agencji ds. ochrony prywatności w ramach administracji federalnej, z zadaniem oceny pod kątem prywatności wszelkich inicjatyw, które mogłyby ją potencjalnie naruszać;
 - b) utworzenia mechanizmu gwarantującego obywatelom USA prawo do odwołania się w razie niewłaściwego wykorzystania ich danych;
6. uważa niemniej, że powyższe ulepszenia są niewystarczające, jeżeli chodzi o ochronę danych obywateli UE przebywających na terenie USA, i że mile widziana byłaby amerykańska podstawa prawna zapewniająca obywatelom europejskim dostęp do swoich danych, w tym ich poprawki i zmiany, oraz dająca możliwość odwołania się do mechanizmu prawnego lub niezależnego organu ochrony danych (jak przewiduje konstytucja USA i ustawa o ochronie danych osobowych z 1974 r.);
7. ponownie wyraża przekonanie, że takie gwarancje ochrony danych ułatwiłyby ich udostępnianie przy zachowaniu ochrony prywatności oraz że ich przekazywanie w każdym wypadku powinno opierać się na co najmniej jednej umowie międzynarodowej o strukturze analogicznej do umowy UE-USA o współpracy sądowej w sprawach karnych i o ekstradycji, analizowanej aktualnie przez Kongres USA;

Środa, 14 lutego 2007 r.

8. uważa, że o ile umowy międzynarodowe dotyczą praw podstawowych zarówno obywateli UE, jak i USA, w prace należy w pełni zaangażować Parlament Europejski i parlamenty krajowe państw członkowskich, podobnie jak Kongres USA;
9. podkreśla, że w kwestii ochrony danych należy starać się, aby umowy zapewniały wysoki poziom ochrony danych w związku z ryzykiem nadużyć i były uzupełnione wiążącymi zasadami na szczeblu UE dotyczącymi ochrony danych w celach bezpieczeństwa (trzeci filar);
10. podkreśla konieczność przyjęcia decyzji ramowej w sprawie ochrony danych osobowych w trzecim filarze; przypomina, że w swoim stanowisku przyjętym jednogłośnie w dniu 27 września 2006 r.⁽¹⁾ Parlament Europejski zaapelował o kompleksowe i ambitne ramy ustanawiające przepisy w zakresie ochrony danych, w tym wymiany danych osobowych z krajami trzecimi;
11. uważa, że należy określić, we współpracy z USA, wspólne ramy ochrony niezbędnych gwarancji, których wymaga szczególne partnerstwo UE-USA w walce z terroryzmem, a które mogłyby także obejmować wszystkie aspekty związane ze swobodnym przepływem osób między UE i USA;
12. oczekuje, że niniejsza strategia partnerstwa transatlantyckiego będzie przedyskutowana na kolejnym szczycie UE-USA w dniu 30 kwietnia 2007 r., oraz zauważa, że w tym kontekście potrzebne jest wzmocnienie kontaktów między Parlamentem Europejskim a Kongresem; wnosi:
- aby sprawozdawcy z Parlamentu Europejskiego uczestniczyli w przesłuchaniu w Kongresie USA na tematy budzące wzajemne zainteresowanie (umowa UE-USA o współpracy sądowej w sprawach karnych i o ekstradycji, ATS, SWIFT);
 - aby wystosować zaproszenie do przewodniczących właściwych komisji Kongresu w perspektywie kolejnego dialogu transatlantyckiego (Bruksela-Berlin, połowa kwietnia 2007 r.), a w każdym razie nie później niż przed kolejnym wiosennym szczytem UE-USA;

Negocjacje w sprawie długoterminowego porozumienia dotyczącego PNR

13. podkreśla, że poza punktami przyjętymi przez Parlament w swoim stanowisku z dnia 27 września 2006 r. przyszłe długoterminowe porozumienie dotyczące PNR powinno przestrzegać następujących zasad:
- kształtowania polityk w oparciu o fakty: przed zawarciem nowego porozumienia niezbędne jest przeprowadzenie wnikliwej analizy faktów; należy rozpatrzyć kwestię skuteczności obecnego (oraz byłego) porozumienia oraz kwestię kosztów i konkurencyjności europejskich przewoźników lotniczych; ocena powinna obejmować realizację zobowiązań oraz kwestie związane z danymi PNR przechowywanymi w systemie automatycznego naprowadzania (ATS);
 - przekazywania danych dotyczących pasażerów (PNR) w oparciu o jasno określony, ograniczony cel;
 - uzasadnienia i proporcjonalności: wydaje się, że w praktyce dane danymi systemu informatycznego przekazywania informacji o pasażerach (APIS) są w zupełności wystarczające dla egzekwowania prawa i bezpieczeństwa; zgodnie z rozporządzeniem Rady (EWG) nr 2299/89 z dnia 24 lipca 1989 w sprawie kodeksu postępowania dla komputerowych systemów rezerwacji w Europie⁽²⁾ gromadzi się już te dane, co umożliwia wymianę z USA w ramach porównywalnego systemu; zebrane w PNR dane dotyczące zachowania wydają się mieć ograniczone zastosowanie, ponieważ nie można ich zidentyfikować bez połączenia z APIS; zatem powody uzasadniające potrzebę przekazywania wszystkich danych PNR są niewystarczające;
 - przyszłe porozumienie musi przestrzegać zasady adekwatności w kontekście ochrony danych osobowych; UE doskonale zdaje sobie sprawę z pilnej potrzeby określenia reguł ochrony danych osobowych w trzecim filarze oraz ustalenia światowych norm obejmujących wszystkie kategorie danych osobowych;
 - konieczne jest przeprowadzanie regularnej oceny adekwatności ochrony danych oraz skuteczności programu, włączając w ten proces Parlament Europejski i w miarę możliwości Kongres USA; ocena roczna musi stać się częścią przyszłego porozumienia; sprawozdanie z oceny należy podać do wiadomości publicznej oraz przekazać Parlamentowi Europejskiemu;
 - rozwiązania alternatywne, takie jak elektroniczne zezwolenie na podróż w ramach programu bezwizowego, zastępujące przekazywanie danych PNR przez towarzystwa lotnicze, również muszą być zgodne z normami ochrony danych UE;

⁽¹⁾ Teksty przyjęte, P6_TA(2006)0370.

⁽²⁾ Dz.U. L 220 z 29.7.1989, str. 1.

Środa, 14 lutego 2007 r.

- g) zasady określone obecnie dla amerykańskich przedsiębiorstw muszą stanowić integralną część porozumienia i być prawnie wiążące; należy zwiększyć legitymację demokratyczną przyszłego porozumienia poprzez pełen udział Parlamentu Europejskiego i/lub ratyfikację przez parlamenty krajowe;
- h) przyszłe porozumienie musi się bezwzględnie opierać na systemie „PUSH”, natomiast system „PULL” należy wyeliminować, pamiętając, że system „PUSH” powinien być już wprowadzony w poprzednim porozumieniu, w momencie gdy było to technicznie wykonalne;
- i) pasażerowie powinni być informowani o przekazaniu danych PNR oraz mieć dostęp do swoich danych, łącznie z poprawkami i zmianami; powinni być również uprawnieni do korzystania z mechanizmów prawnych lub zwrócenia się do niezależnego organu ochrony danych;
- j) oczekuje, że władze USA w przypadku potwierdzonego zagrożenia terrorystycznego są zobowiązane do niezwłocznego poinformowania władz UE o tym podejrzeniu;

Dostęp do danych SWIFT

14. potwierdza swoje zaniepokojenie faktem, że od czterech lat w ramach systemu SWIFT, w wyniku decyzji SWIFT opartej na systemowych i handlowych przesłankach wynikających z chęci systematycznego kopiowania danych do analogicznego systemu w USA, przy odbiorze wezwań do sądu przekazywano administracji USA podzbiór danych przetwarzanych w systemie SWIFT w USA, w tym do danych nie dotyczących obywateli USA oraz danych zebranych poza terytorium Stanów Zjednoczonych, naruszając tym samym prawo ochrony danych UE;

15. uważa za niezwykle niepokojące, że powyższe praktyki, sprzeczne z Europejską Konwencją Ochrony Praw Człowieka i Podstawowych Wolności, Kartą Praw Podstawowych Unii Europejskiej oraz z traktatami i prawem pochodnym (dyrektywa o ochronie danych oraz rozporządzenie (WE) nr 45/2001 Parlamentu Europejskiego i Rady z dnia 18 grudnia 2000 r. o ochronie osób fizycznych w związku z przetwarzaniem danych osobowych przez instytucje i organy wspólnotowe i o swobodnym przepływie takich danych⁽¹⁾), nie zostały wcześniej zdecydowanie skrytykowane ani przez Europejski Bank Centralny, ani przez grupę 10 banków nadzorujących system SWIFT, oraz że europejskie banki oraz ich klienci dopiero niedawno dowiedzieli się o istniejącej sytuacji z prasy;

16. wyraża ubolewanie z powodu faktu, że parę miesięcy po ujawnieniu wyżej wspomnianych praktyk Rada nie zajęła jeszcze żadnego stanowiska w kwestii, która dotyczy przecież tak wielu obywateli, konsumentów, przedsiębiorstw, oraz że tylko siedem spośród 27 państw członkowskich odpowiedziało na przekazaną im przez Komisję Europejską ankietę mającą na celu zebranie wyjaśnień na temat wspólnotowego oraz krajowego prawodawstwa dotyczącego ochrony danych;

17. ponownie wyraża zaniepokojenie obecnym systemem kontroli SWIFT, za który odpowiedzialność ponosi grupa 10 banków centralnych z nadzorem przez EBC, nie mając jednak żadnych oficjalnych uprawnień; wzywa Radę i EBC do wspólnego rozważenia metod ulepszenia systemu celem zapewnienia prawidłowego funkcjonowania procesu wprowadzania wpisów ze wszystkimi konsekwencjami w zakresie podejmowanych działań;

18. popiera opinię Europejskiego Inspektora Ochrony Danych na temat roli Europejskiego Banku Centralnego oraz wzywa EBC:

- jako nadzorcę systemu SWIFT, do znalezienia rozwiązań zapewniających zgodność z przepisami dotyczącymi ochrony danych osobowych oraz do zagwarantowania, że zasady dotyczące poufności nie będą przeszkodą w sprawnym informowaniu odpowiednich władz;
- jako użytkownika SWIFTNet-FIN, do znalezienia rozwiązań zapewniających zgodność operacji płatniczych z przepisami dotyczącymi ochrony danych osobowych, i przygotowania, najpóźniej do kwietnia 2007 r., sprawozdania na temat środków do podjęcia;
- jako decydenta, do zapewnienia, we współpracy z bankami centralnymi i instytucjami finansowymi, pełnej zgodności europejskich systemów opłat, w tym uaktualnionego systemu płatności w handlu hurtowym TARGET2, oraz planowanego systemu dla papierów wartościowych TARGET, w razie jego urzeczywistnienia, z prawem ochrony danych UE;

(¹) Dz.U. L 8 z 12.1.2001, str. 1.

Środa, 14 lutego 2007 r.

19. ponownie wyraża nadzieję, że pod ściśle określonymi warunkami dane zebrane podczas transakcji finansowych będą mogły być wykorzystane wyłącznie w postępowaniu sądowym w przypadkach podejrzeń o finansowanie terroryzmu, oraz przypomina, że zarówno UE, jak i USA wdrożyły w swoim ustawodawstwie zalecenie VII Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy (rozporządzenie (WE) nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie informacji o zlecceniodawcach, które towarzyszą przekazom pieniężnym⁽¹⁾ oraz ustawa USA o tajemnicy bankowej);

20. przypomina, że zgodnie z zaleceniem VII grupy Grupy Specjalnej ds. Przeciwdziałania Praniu Pieniędzy, od dnia 31 grudnia 2006 r., instytucje finansowe mają obowiązek gromadzenia oraz przechowywania pewnych określonych rodzajów danych dotyczących przekazów pieniężnych w Europie na kwotę od 1000 USD (w USA 3000 USD); dane te są przekazywane lub udostępniane na wniosek władzom⁽²⁾;

21. wierzy, że UE i USA są głównymi i lojalnymi sojusznikami w walce z terroryzmem, a zatem podstawą dla negocjacji na temat możliwego porozumienia międzynarodowego powinny być ustalone ramy prawne, w oparciu o założenie, że SWIFT jako przedsiębiorstwo belgijskie podlega prawu Belgii i jest w związku z tym zobowiązane do przetwarzania danych zgodnie z art. 4 ust. 2 dyrektywy 95/46/WE; naturalną konsekwencją byłoby zatem zakazanie przedsiębiorstwu prowadzenia obecnych praktyk kopiowania wszystkich danych dotyczących obywateli UE i przedsiębiorstw do swojego systemu w USA, lub przeniesienia alternatywnej bazy danych poza jurysdykcję USA; należa, aby wyżej wspomniane porozumienie dostarczało niezbędnych gwarancji zapobiegających prowadzącemu do nadużyć wykorzystywaniu danych w celach gospodarczych i handlowych;

22. zwraca uwagę na fakt, że SWIFT świadczy usługi poza UE oraz w Stanach Zjednoczonych, a zatem każdy przyjęty środek powinien uwzględniać globalny charakter tych usług;

23. wzywa Komisję, której uprawnienia obejmują zarówno ochronę danych, jak i systemy opłat, do rozpatrzenia możliwości szpiegostwa ze szkodą dla gospodarki i przedsiębiorstw wynikającego z obecnego kształtu systemu opłat w najszerszym tego słowa znaczeniu, łącznie z poinformowaniem o tym fakcie dostawców i zaproponowaniem rozwiązań;

24. odnotowuje, że usługi finansowe mogą zostać wyłączone z zakresu porozumienia w sprawie bezpieczeństwa w portach, zgodnie z opinią nr 10/2006 grupy roboczej ds. art. 29; jest zaniepokojony faktem, że przedsiębiorstwa i sektory UE prowadzące działalność w USA i nieobjęte porozumieniem w sprawie bezpieczeństwa w portach mogą być obecnie zmuszane do udostępniania danych osobowych władzom USA, w szczególności amerykańskim oddziałom europejskich banków, zakładom ubezpieczeń, instytucjom opieki społecznej oraz dostawcom usług telekomunikacyjnych; wzywa Komisję Europejską do zbadania tej sytuacji;

*
* *

25. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji oraz rządowi i parlamentom państw członkowskich oraz Kongresowi USA.

⁽¹⁾ Dz.U. L 345 z 8.12.2006, str. 1.

⁽²⁾ (patrz sprawozdanie opublikowane w dniu 17 stycznia 2006 r. przez Sieć ds. ścigania przestępstw finansowych (FinCEN) w sprawie transgranicznych przekazów pieniężnych: http://www.fincen.gov/news_release_cross_border.html).

P6_TA(2007)0040

Strategia lizbońska (Rada Europejska 8-9 marca 2007 r.)

Rezolucja Parlamentu Europejskiego w sprawie wkładu do wiosennego posiedzenia Rady w 2007 r. w związku ze strategią lizbońską

Parlament Europejski,

— uwzględniając komunikat Komisji na wiosenną Radę Europejską zatytułowany „Czas wrzucić wyższy bieg: Nowe partnerstwo na rzecz wzrostu gospodarczego i zatrudnienia (COM(2006)0030),”