|  |  |
| --- | --- |
| Parlament Europejski2014-2019 |  |

Dokument z posiedzenia

<NoDocSe>B8‑0305/2018</NoDocSe>

<Date>{26/06/2018}26.6.2018</Date>

<TitreType>PROJEKT REZOLUCJI</TitreType>

<TitreSuite>złożony w następstwie oświadczenia Komisji</TitreSuite>

<TitreRecueil>zgodnie z art. 123 ust. 2 Regulaminu</TitreRecueil>

<Titre>w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA</Titre>

<DocRef>(2018/2645(RSP))</DocRef>

<RepeatBlock-By><Depute>Claude Moraes</Depute>

<Commission>{LIBE}w imieniu Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych</Commission>

</RepeatBlock-By>

B8‑0305/2018

Rezolucja Parlamentu Europejskiego w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA

(2018/2645(RSP))

*Parlament Europejski*,

– uwzględniając Traktat o Unii Europejskiej (TUE), Traktat o funkcjonowaniu Unii Europejskiej (TFUE) oraz art. 6, 7, 8, 11, 16, 47 i 52 Karty praw podstawowych Unii Europejskiej,

– uwzględniając rozporządzenie (UE) 2016/679 Parlamentu Europejskiego i Rady z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE („ogólne rozporządzenie o ochronie danych”)[[1]](#footnote-1), a także dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych przez właściwe organy do celów zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania i ścigania czynów zabronionych i wykonywania kar, w sprawie swobodnego przepływu takich danych oraz uchylającą decyzję ramową Rady 2008/977/WSiSW[[2]](#footnote-2),

– uwzględniając wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 6 października 2015 r. w sprawie C-362/14 *Maximillian Schrems przeciwko Data Protection Commissioner*[[3]](#footnote-3),

– uwzględniając wyrok Trybunału Sprawiedliwości Unii Europejskiej z dnia 21 grudnia 2016 r. w sprawach C-203/15 *Tele2 Sverige AB przeciwko Post- och telestyrelsen* oraz C-698/15 *Secretary of State for the Home Department przeciwko Tomowi Watsonowi i in.*[[4]](#footnote-4),

– uwzględniając decyzję wykonawczą Komisji (UE) 2016/1250 przyjętą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA[[5]](#footnote-5),

– uwzględniając opinię Europejskiego Inspektora Ochrony Danych (EIOD) nr 4/2016 w sprawie projektu decyzji w sprawie odpowiedniej ochrony danych osobowych w ramach unijno-amerykańskiej ochrony prywatności (*Privacy Shield*)[[6]](#footnote-6),

– uwzględniając opinię Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupy Roboczej Art. 29) nr 01/2016 z dnia 13 kwietnia 2016 r. w sprawie projektu decyzji stwierdzającej odpowiedni stopień ochrony w odniesieniu do Tarczy Prywatności UE-USA[[7]](#footnote-7) oraz oświadczenie tej grupy z dnia 26 lipca 2016 r.[[8]](#footnote-8),

– uwzględniając sprawozdanie Komisji dla Parlamentu Europejskiego i Rady w sprawie pierwszego rocznego przeglądu funkcjonowania Tarczy Prywatności UE-USA[[9]](#footnote-9) oraz dokument roboczy służb Komisji towarzyszący temu sprawozdaniu[[10]](#footnote-10),

– uwzględniając dokument Grupy Roboczej ds. Ochrony Osób Fizycznych w zakresie Przetwarzania Danych Osobowych (Grupy Roboczej Art. 29) z dnia 28 listopada 2017 r. pt. „EU-US Privacy Shield – First Annual Joint Review” [Tarcza Prywatności UE-USA – pierwszy roczny wspólny przegląd][[11]](#footnote-11),

– uwzględniając pismo Grupy Roboczej Art. 29 z dnia 11 kwietnia 2018 r. stanowiące odpowiedź na ponowne zatwierdzenie sekcji 702 ustawy o kontroli wywiadu (FISA) obowiązującej w USA,

– uwzględniając swoją rezolucję z dnia 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez tzw. Tarczę Prywatności UE-USA[[12]](#footnote-12),

– uwzględniając art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 6 października 2015 r. w sprawie C-362/14 *Maximillian Schrems przeciwko Data Protection Commissioner* stwierdził nieważność decyzji w sprawie „bezpiecznej przystani” i wyjaśnił, że odpowiedni stopień ochrony w państwie trzecim należy rozumieć jako „merytorycznie równoważny” stopniowi ochrony gwarantowanemu w Unii Europejskiej na mocy dyrektywy 95/46 w związku z kartą, co pociąga za sobą potrzebę zakończenia negocjacji w sprawie nowego uzgodnienia, tak aby zapewnić pewność prawa co do tego, jak należy przekazywać dane osobowe z UE do USA;

B. mając na uwadze, że przy badaniu stopnia ochrony zapewnianej przez państwo trzecie Komisja zobowiązana jest ocenić treść przepisów obowiązujących w tym państwie wynikających z jego prawa krajowego lub zobowiązań międzynarodowych, a także praktyk mających na celu zapewnienie zgodności z tymi przepisami, gdyż na mocy art. 25 ust. 2 dyrektywy 95/46/WE musi ona uwzględnić wszystkie okoliczności dotyczące przekazywania danych osobowych do państwa trzeciego; mając na uwadze, że ocena ta musi odnosić się nie tylko do przepisów i praktyk związanych z ochroną danych osobowych do celów handlowych i prywatnych, ale musi również obejmować wszystkie aspekty ram prawnych mających zastosowanie do tego kraju lub sektora – w szczególności, lecz nie tylko, egzekwowanie prawa, bezpieczeństwo narodowe i poszanowanie praw podstawowych;

C. mając na uwadze, że przekazywanie danych osobowych między organizacjami handlowymi z UE i z USA stanowi ważny element stosunków transatlantyckich w kontekście stale postępującej cyfryzacji globalnej gospodarki; mając na uwadze, że przekazywanie tych danych powinno odbywać się przy pełnym poszanowaniu prawa do ochrony danych osobowych oraz prawa do prywatności; mając na uwadze, że jednym z podstawowych celów UE jest ochrona praw podstawowych zapisanych w karcie;

D. mając na uwadze, że Facebook, który jest jednym z sygnatariuszy Tarczy Prywatności, potwierdził, że dane 2,7 mln obywateli Unii znalazły się wśród danych niewłaściwie wykorzystywanych przez agencję doradztwa politycznego Cambridge Analytica;

E. mając na uwadze, że w opinii nr 4/2016 EIOD dał wyraz wielu obawom dotyczącym projektu Tarczy Prywatności; mając na uwadze, że w tej samej opinii EIOD przyjmuje z zadowoleniem działania podejmowane przez strony na rzecz znalezienia rozwiązania na potrzeby przekazywania danych osobowych z UE do Stanów Zjednoczonych w celach handlowych w ramach systemu autocertyfikacji;

F. mając na uwadze, że w opinii nr 01/2016 w sprawie projektu decyzji wykonawczej w sprawie adekwatności Tarczy Prywatności UE-USA Grupa Robocza Art. 29 przyjęła z zadowoleniem poprawę wynikającą z Tarczy Prywatności w porównaniu z decyzją w sprawie zasady „bezpiecznej przystani”, jednocześnie wyrażając poważne obawy zarówno o aspekty handlowe, jak i o kwestię dostępu organów publicznych do danych przekazywanych w ramach Tarczy Prywatności;

G. mając na uwadze, że w dniu 12 lipca 2016 r., po dalszych dyskusjach z administracją USA, Komisja przyjęła decyzję wykonawczą (UE) 2016/1250, stwierdzając odpowiedni stopień ochrony danych osobowych przekazywanych z Unii do organizacji w Stanach Zjednoczonych w ramach Tarczy Prywatności UE-USA;

H. mając na uwadze, że Tarczy Prywatności UE-USA towarzyszy szereg jednostronnych zobowiązań i zapewnień administracji USA wyjaśniających m.in. zasady ochrony danych, sposób prowadzenia nadzoru, egzekwowanie prawa i ochronę prawną, a także środki ochrony i zabezpieczenia, w oparciu o które agencje bezpieczeństwa mogą uzyskać dostęp do danych osobowych oraz przetwarzać te dane;

I. mając na uwadze, że w oświadczeniu z dnia 26 lipca 2016 r. Grupa Robocza Art. 29 przyjmuje z zadowoleniem usprawnienia, jakie przyniósł mechanizm Tarczy Prywatności UE-USA w porównaniu z zasadą „bezpiecznej przystani”, oraz wyraziła uznanie dla Komisji i władz USA za uwzględnienie jej obaw; mając na uwadze, że Grupa Robocza Art. 29 mimo to zwraca uwagę, iż wciąż nie rozwiano wiele jej obaw, odnoszących się do zarówno aspektów handlowych, jak i dostępu organów publicznych USA do danych przekazywanych z UE, w tym do kwestii braku przepisów szczegółowych dotyczących zautomatyzowanego podejmowania decyzji oraz ogólnego prawa do wyrażenia sprzeciwu, potrzeby bardziej rygorystycznych gwarancji, jeśli chodzi o niezależność i uprawnienia mechanizmu Rzecznika ds. Tarczy Prywatności, czy też braku konkretnych gwarancji, że dane osobowe nie będą gromadzone w sposób powszechny i bezkrytyczny (hurtowe gromadzenie danych);

J. mając na uwadze, że choć w swojej rezolucji z dnia 6 kwietnia 2017 r. Parlament Europejski uznał, iż Tarcza Prywatności UE-USA stanowi znaczne usprawnienie, jeśli chodzi o przejrzystość norm, w stosunku do wcześniejszej zasady bezpiecznej przystani UE-USA, jednocześnie stwierdził, że bez odpowiedzi pozostają ważne pytania co do pewnych aspektów handlowych, bezpieczeństwa narodowego oraz egzekwowania prawa; mając na uwadze, że Parlament wzywa Komisję, by podczas pierwszego wspólnego przeglądu rocznego przeprowadziła szczegółową i dogłębną analizę wszystkich niedociągnięć i słabych punktów, a także poinformowała, jakie podjęto w związku z nimi działania, by zapewnić zgodność z kartą oraz prawem Unii, jak również by szczegółowo przeanalizowała, czy mechanizmy i zabezpieczenia wskazane w gwarancjach i wyjaśnieniach administracji USA są skuteczne i wykonalne;

K. mając na uwadze, że choć w sprawozdaniu Komisji dla Parlamentu Europejskiego i Rady w sprawie pierwszego rocznego przeglądu funkcjonowania Tarczy Prywatności UE-USA oraz w dokumencie roboczym służb Komisji towarzyszącym temu sprawozdaniu stwierdzono, że władze USA ustanowiły niezbędne struktury i procedury w celu zapewnienia właściwego funkcjonowania Tarczy Prywatności, oraz zawarto wniosek, że USA nadal zapewniają odpowiedni stopień ochrony danych osobowych przekazywanych w ramach Tarczy, jednocześnie sformułowano w nich dziesięć zaleceń dla władz USA w celu usunięcia budzących niepokój kwestii dotyczących nie tylko zadań i działań Departamentu Handlu USA jako organu zarządzającego właściwego ds. monitorowania certyfikacji organizacji w ramach Tarczy Prywatności i egzekwowania zasad jej funkcjonowania, ale także kwestii związanych z bezpieczeństwem narodowym, takich jak ponowne zatwierdzenie sekcji 702 ustawy o kontroli wywiadu (FISA) czy mianowanie stałego Rzecznika ds. Tarczy Prywatności i fakt, że wciąż nie zostali mianowani członkowie Rady Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (PCLOB);

L. mając na uwadze, że w przyjętej w dniu 28 listopada 2017 r. opinii Grupy Roboczej Art. 29 pt. „Tarcza Prywatności UE-USA – pierwszy wspólny przegląd roczny”, którą sporządzono na podstawie pierwszego wspólnego przeglądu rocznego, przyjęto do wiadomości postęp, jakim jest Tarcza Prywatności w porównaniu z unieważnioną decyzją w sprawie zasady „bezpiecznej przystani”; mając na uwadze, że Grupa Robocza Art. 29 uznaje działania podejmowane przez władze USA i Komisję na rzecz wdrożenia Tarczy Prywatności;

M. mając na uwadze, że Grupa Robocza Art. 29 wskazała szereg ważnych nierozwiązanych i budzących poważne obawy kwestii dotyczących aspektów handlowych i aspektów związanych z dostępem amerykańskich organów publicznych do danych przekazywanych do USA w ramach Tarczy Prywatności (do celów egzekwowania prawa lub bezpieczeństwa narodowego), którymi to kwestiami muszą zająć się zarówno Komisja, jak i władze USA; mając na uwadze, że grupa zwróciła się o niezwłoczne opracowanie planu działania w celu zapewnienia, by wszystkie te obawy zostały wyeliminowane, oraz o to, by stało się to najpóźniej w ramach drugiego wspólnego przeglądu;

N. mając na uwadze, że jeśli w określonych ramach czasowych nie uda się wyeliminować obaw wyrażonych przez Grupę Roboczą Art. 29, członkowie tej grupy podejmą odpowiednie działania, w tym zaskarżą decyzję stwierdzającą odpowiedni stopień ochrony w odniesieniu do Tarczy Prywatności przed sądami krajowymi, aby te wystąpiły z wnioskiem do Trybunału Sprawiedliwości Unii Europejskiej o wydanie orzeczenia w trybie prejudycjalnym;

O. mając na uwadze, że skarga o stwierdzenie nieważności (sprawa T-738/16 *La Quadrature du Net i inni przeciwko Komisji*) oraz wniosek Sądu Najwyższego Irlandii o wydanie opinii w sprawie toczącej się między irlandzkim urzędem Data Protection Commissioner a spółką Facebook Ireland Limited i Maximilianem Schremsem (sprawa *Schrems II*) zostały skierowane do Trybunału Sprawiedliwości Unii Europejskiej; mając na uwadze, że we wniosku o wydanie opinii uwzględniono fakt, iż nadal ma miejsce masowa inwigilacja, oraz przeanalizowano, czy w prawie USA istnieją skuteczne środki odwoławcze chroniące obywateli Unii, których dane osobowe są przekazywane do Stanów Zjednoczonych;

P. mając na uwadze, że w dniu 11 stycznia 2018 r. Kongres Stanów Zjednoczonych ponownie zatwierdził oraz znowelizował sekcję 702 ustawy o kontroli wywiadu na okres sześciu lat, nie odnosząc się do obaw przedstawionych w sprawozdaniu Komisji dotyczącym wspólnego przeglądu oraz w opinii Grupy Roboczej Art. 29;

Q. mając na uwadze, że w ramach zbiorczych przepisów budżetowych wprowadzonych w życie w dniu 23 marca 2018 r. Kongres Stanów Zjednoczonych przyjął ustawę wyjaśniającą kwestię transgranicznego wykorzystywania danych (tzw. ustawę „CLOUD”), która ułatwia organom egzekwowania prawa dostęp do treści korespondencji i innych powiązanych danych, zezwalając organom egzekwowania prawa w USA na wydawanie nakazów ujawniania danych pochodzących z korespondencji, nawet jeśli są one przechowywane poza Stanami Zjednoczonymi, oraz umożliwiając niektórym państwom trzecim zawieranie umów wykonawczych ze Stanami Zjednoczonymi pozwalających dostawcom usług z USA na udzielanie odpowiedzi na nakazy z określonych państw trzecich dotyczące uzyskania dostępu do danych pochodzących z korespondencji;

R. mając na uwadze, że Facebook Inc., Cambridge Analytica oraz SCL Elections Ltd są spółkami certyfikowanymi w ramach Tarczy Prywatności i jako takie wykorzystywały decyzję stwierdzającą odpowiedni stopień ochrony jako podstawę prawną do przekazywania danych osobowych z Unii Europejskiej do Stanów Zjednoczonych i do dalszego przetwarzania tych danych;

S. mając na uwadze, że jeżeli – zgodnie z art. 45 ust. 5 RODO – dostępne informacje wskazują, że państwo trzecie przestało zapewniać odpowiedni stopień ochrony, Komisja uchyla, zmienia lub zawiesza swoją decyzję stwierdzającą odpowiedni stopień ochrony;

1. podkreśla nieusunięte jeszcze niedociągnięcia Tarczy Prywatności w odniesieniu do praw podstawowych osób, których dane dotyczą; zwraca uwagę na coraz większe ryzyko, że Trybunał Sprawiedliwości Unii Europejskiej stwierdzi nieważność decyzji wykonawczej Komisji (UE) 2016/1250 w sprawie Tarczy Prywatności;

2. odnotowuje usprawnienia osiągnięte w porównaniu z porozumieniem w sprawie „bezpiecznej przystani”, w tym włączenie kluczowych definicji, bardziej rygorystyczne obowiązki dotyczące zatrzymywania danych i dalszego ich przekazywania do państw trzecich, utworzenie mechanizmu Rzecznika ds. Tarczy Prywatności w celu zapewnienia indywidualnych środków ochrony prawnej i niezależnego nadzoru, mechanizmy kontroli i równowagi gwarantujące prawa osób, których dane dotyczą (PCLOB), zewnętrzne i wewnętrzne przeglądy zgodności, bardziej regularne i rygorystyczne dokumentowanie i monitorowanie, dostępność kilku ścieżek ochrony prawnej, a także przyznanie nadrzędnej roli krajowym organom ochrony danych w zakresie prowadzenia dochodzeń w sprawie skarg;

3. przypomina, że Grupa Robocza Art. 29 wyznaczyła dzień 25 maja 2018 r. jako termin rozwiązania utrzymujących się problemów, przy czym w przypadku niedotrzymania tego terminu Grupa Robocza Art. 29 może podjąć decyzję o zaskarżeniu Tarczy Prywatności, kierując sprawę do sądów krajowych, aby te wystąpiły z wnioskiem do Trybunału Sprawiedliwości Unii Europejskiej o wydanie orzeczenia w trybie prejudycjalnym[[13]](#footnote-13);

**Kwestie instytucjonalne / Obsadzanie stanowisk**

4. wyraża ubolewanie, że wyznaczenie dwójki dodatkowych członków wraz z powołaniem przewodniczącego PCLOB zajęło tak wiele czasu, oraz wzywa Senat do przeprowadzenia kontroli tych kandydatur w celu zatwierdzenia ich nominacji, tak aby ta niezależna agencja odzyskała kworum i mogła wykonywać powierzone jej zadania z zakresu zapobiegania terroryzmowi i gwarantowania ochrony prywatności i swobód obywatelskich;

5. wyraża zaniepokojenie faktem, że brak przewodniczącego i brak kworum ograniczyły zdolność PCLOB do działania i wypełniania obowiązków; podkreśla, że w okresie braku kworum PCLOB nie może podejmować się nowych projektów z zakresu doradztwa lub nadzoru ani nie może zatrudniać personelu; przypomina, że PCLOB nie opublikował jeszcze długo oczekiwanego sprawozdania dotyczącego prowadzenia inwigilacji na podstawie dekretu 12333 w celu przedstawienia informacji na temat konkretnego wykonywania tego dekretu oraz jego konieczności i proporcjonalności w kontekście zakłóceń wywołanych w związku z tym dekretem w dziedzinie ochrony danych; zauważa, że sprawozdanie to jest wysoce pożądane, zważywszy na niepewność i nieprzewidywalność w związku z tym jak dekret 12333 jest stosowany; ubolewa, że PCLOB nie opublikowała nowego sprawozdania w sprawie sekcji 702 ustawy o kontroli wywiadu przed ponownym zatwierdzeniem tej sekcji w styczniu 2018 r.; uważa, że sytuacja braku kworum w poważnym stopniu niweczy gwarancje i zapewnienia w zakresie zgodności i nadzoru składane przez władze USA; wzywa w związku z tym władze USA do niezwłocznego nominowania i zatwierdzenia członków rady;

6. w świetle faktu, że dyrektywa polityczna Prezydenta nr 28 stanowi jeden z głównych elementów, na których zbudowana jest Tarcza Prywatności, apeluje o ujawnienie sprawozdania PCLOB dotyczącego tej dyrektywy, które nadal objęte jest przywilejem prezydenckim i w związku z tym nie zostało dotychczas opublikowane;

7. powtarza swoje stanowisko, że mechanizm Rzecznika ds. Tarczy Prywatności wprowadzony przez Departament Stanu USA nie jest wystarczająco niezależny ani nie jest wyposażony w wystarczające uprawnienia faktyczne umożliwiające realizację jego zadań i zapewnianie obywatelom Unii skutecznych środków ochrony prawnej; podkreśla, że dokładny zakres uprawnień mechanizmu Rzecznika ds. Tarczy Prywatności wymaga doprecyzowania, zwłaszcza w odniesieniu do jego uprawnień w dziedzinie struktur wywiadowczych oraz poziomu skutecznych środków odwoławczych od jego decyzji; ubolewa, że Rzecznik ds. Tarczy Prywatności może zwracać się o podjęcie działań i informacje jedynie do organów rządu USA, przy czym nie może nakazać tym organom przerwania i zaprzestania dalszego bezprawnego inwigilowania ani nie może nakazać trwałego zniszczenia informacji; zwraca uwagę, że choć zadania Rzecznika ds. Tarczy Prywatności wypełnia obecnie osoba pełniąca obowiązki rzecznika, administracja USA nie mianowała dotychczas nowego stałego rzecznika, co nie przyczynia się do budowania wzajemnego zaufania; jest zdania, że z uwagi na brak nominacji niezależnego i doświadczonego Rzecznika ds. Tarczy Prywatności o wystarczających uprawnieniach zapewnienia Stanów Zjednoczonych dotyczące zapewnienia obywatelom Unii skutecznej ochrony prawnej należy uznać za deklaracje bez pokrycia;

8. przyjmuje do wiadomości niedawne zatwierdzenie przez Senat nowego przewodniczącego i czterech komisarzy Federalnej Komisji Handlu (FTC); zważywszy na fakt, iż FTC jest agencją właściwą ds. egzekwowania stosowania zasad Tarczy Prywatności przez organizacje w USA, wyraża ubolewanie, że do momentu wspomnianego zatwierdzenia nieobsadzone były cztery z pięciu stanowisk w FTC;

9. podkreśla, że niedawne doniesienia dotyczące praktyk stosowanych przez Facebook i Cambridge Analytica każą zwrócić szczególną uwagę na konieczność podejmowania proaktywnych działań z zakresu nadzoru i egzekwowania, które nie będą bazować jedynie na skargach, ale które będą obejmować systematyczne kontrole zgodności w praktyce polityk z zakresu prywatności z zasadami Tarczy Prywatności w ramach całego cyklu życia certyfikacji; wzywa unijne organy właściwe ds. ochrony danych do podjęcia odpowiednich działań i zawieszenia przekazywania danych w przypadku braku zgodności;

**Kwestie handlowe**

10. uważa, że aby zapewnić przejrzystość i zapobiegać fałszywym informacjom na temat posiadanej certyfikacji, Departament Handlu nie powinien tolerować przypadków, w których amerykańskie spółki publicznie ogłaszają fakt posiadania certyfikacji Tarczy Prywatności jeszcze przed zakończeniem procedury certyfikacji i umieszczeniem ich w wykazie Tarczy Prywatności; jest zaniepokojony faktem, że Departament Handlu nie korzysta z przewidzianej w Tarczy Prywatności możliwości zażądania kopii warunków umownych stosowanych przez certyfikowane spółki w ich umowach ze stronami trzecimi w celu zapewnienia zgodności; uważa w związku z tym, że nie jest prowadzona żadna skuteczna kontrola sprawdzająca, czy certyfikowane spółki faktycznie przestrzegają przepisów Tarczy Prywatności; wzywa Departament Handlu do przeprowadzania w proaktywny i regularny sposób przeglądów z urzędu badających zgodność z przepisami w celu monitorowania faktycznego przestrzegania przez spółki zasad i wymogów określonych w Tarczy Prywatności;

11. uważa, że różne procedury dochodzenia praw przez obywateli Unii mogą okazać się zbyt złożone, trudne do zastosowania, a w związku z tym mniej skuteczne; zauważa, że – jak podkreśliły to przedsiębiorstwa zapewniające mechanizmy niezależnej ochrony prawnej – większość skarg wpływa bezpośrednio do przedsiębiorstw, a składają je osoby fizyczne usiłujące uzyskać ogólne informacje o Tarczy Prywatności i przetwarzaniu ich danych; zaleca zatem władzom USA, aby na stronie internetowej Tarczy Prywatności przedstawiły osobom fizycznym w przystępnej i łatwej do zrozumienia formie bardziej konkretne informacje na temat ich praw oraz dostępnych środków z zakresu dochodzenia roszczeń i procedur odwoławczych;

12. w związku z niedawnymi doniesieniami na temat niewłaściwego wykorzystywania danych osobowych przez przedsiębiorstwa certyfikowane na mocy Tarczy Prywatności, takie jak Facebook czy Cambridge Analytica, wzywa władze USA właściwe ds. egzekwowania przepisów Tarczy Prywatności do niezwłocznego podejmowania działań na podstawie takich doniesień przy pełnym poszanowaniu złożonych zapewnień i zaciągniętych zobowiązań dotyczących utrzymania w mocy obecnego porozumienia w sprawie Tarczy Prywatności oraz, w razie potrzeby, do usuwania takich spółek z wykazu Tarczy Prywatności; wzywa również unijne organy właściwe ds. ochrony danych do badania takich doniesień i, w stosownych przypadkach, do zawieszania lub zakazywania przekazywania danych w ramach Tarczy Prywatności; uważa, że doniesienia te stanowią wyraźny dowód, iż mechanizm Tarczy Prywatności nie zapewnia odpowiedniej ochrony prawa do ochrony danych;

13. wyraża poważne zaniepokojenie dokonaną przez spółkę Facebook zmianą warunków świadczenia usług dla użytkowników spoza UE, z wyłączeniem Stanów Zjednoczonych i Kanady, którym to użytkownikom przysługiwały dotychczas prawa przewidziane w unijnych przepisach o ochronie danych, a którzy muszą obecnie zaakceptować fakt, że administratorem ich danych jest spółka Facebook USA, a nie spółka Facebook Irlandia; uważa, że takie działanie stanowi przekazanie danych osobowych ok. 1,5 mld użytkowników państwu trzeciemu; mocno wątpi w to, że takie bezprecedensowe i zakrojone na dużą skalę ograniczenie praw podstawowych użytkowników platformy będącej *de facto* monopolistą jest zmierzaniem w kierunku celu, który przyświeca Tarczy Prywatności; wzywa unijne organy właściwe ds. ochrony danych do zbadania tej sprawy;

14. wyraża głębokie zaniepokojenie tym, że jeśli kwestia ta nie zostanie wyjaśniona, takie niewłaściwe wykorzystywanie danych osobowych obywateli przez różne podmioty, których celem jest manipulowanie ich opiniami politycznymi lub postawą podczas wyborów, może zagrozić systemowi demokratycznemu oraz leżącej u jego podstaw idei, że wyborcy mogą samodzielnie dokonywać świadomych decyzji w oparciu o fakty;

15. przyjmuje z zadowoleniem i popiera apele skierowane do ustawodawcy w Stanach Zjednoczonych o przyjęcie zbiorczego aktu prawnego dotyczącego ochrony prywatności i danych;

16. przypomina swoje obawy co do braku w ramach Tarczy Prywatności szczególnych przepisów i gwarancji dotyczących decyzji podejmowanych na podstawie zautomatyzowanego przetwarzania/profilowania, które wywołują skutki prawne lub wywierają znaczący wpływ na daną osobę fizyczną; przyjmuje do wiadomości zamiar Komisji dotyczący zamówienia badania mającego na celu zgromadzenie udokumentowanych informacji, a następnie dokonanie oceny odpowiedniości zautomatyzowanego procesu decyzyjnego w zakresie przekazywania danych w ramach Tarczy Prywatności; wzywa Komisję do zapewnienia – jeśli we wspomnianym badaniu zostaną sformułowane zalecenia w tym zakresie – szczególnych zasad dotyczących zautomatyzowanego procesu decyzyjnego, tak aby gwarantował on wystarczające zabezpieczenia; w związku z powyższym przyjmuje do wiadomości informacje zawarte we wspólnym przeglądzie, z którego wynika, że zautomatyzowany proces decyzyjny nie może odbywać się na podstawie danych osobowych, które zostały przekazane w ramach Tarczy Prywatności; ubolewa jednak nad faktem, że według Grupy Roboczej Art. 29 „informacje zwrotne od przedsiębiorstw utrzymywały się na poziomie dużej ogólności, pozostawiając niejasność co do tego, czy te zapewnienia znajdują potwierdzenie w rzeczywistej sytuacji we wszystkich przedsiębiorstwach uczestniczących w ramach Tarczy Prywatności”; podkreśla ponadto stosowanie RODO zgodnie z warunkami określonymi w art. 3 ust. 2 RODO;

17. podkreśla, że dalsze usprawnienia powinny dotyczyć kwestii interpretacji i przetwarzania danych dotyczących zasobów ludzkich ze względu na odmienne pojmowanie terminu „dane dotyczące zasobów ludzkich” przez rząd USA z jednej strony oraz przez Komisję Europejską i Grupę Roboczą Art. 29 z drugiej strony; w pełni zgadza się z apelem wystosowanym przez Grupę Roboczą Art. 29 do Komisji Europejskiej, aby zaangażowała się ona w negocjacje z władzami USA mające na celu zmianę mechanizmu Tarczy Prywatności w tym zakresie;

18. ponownie wyraża zaniepokojenie faktem, że zasady Tarczy Prywatności nie idą śladem unijnego modelu przetwarzania danych opartym na wyrażeniu zgody, ale przewidują możliwość zastosowania klauzuli opt-out / prawa wniesienia sprzeciwu jedynie w bardzo szczególnych okolicznościach; apeluje w związku z tym, aby w świetle wspólnego przeglądu Departament Handlu współpracował z europejskimi organami ochrony danych w celu opracowania bardziej precyzyjnych wytycznych dotyczących istotnych zasad Tarczy Prywatności, takich jak zasada wyboru, zasada powiadamiania, dalsze przekazywanie danych, stosunek między administratorem a podmiotem przetwarzającym oraz dostęp, które to zasady będą dużo bardziej dostosowane do praw osób, których dane dotyczą, określonych w rozporządzeniu (UE) 2016/679;

19. ponownie wyraża zaniepokojenie z powodu odrzucenia przez Kongres w marcu 2017 r. zasady zaproponowanej przez Federalną Komisję Łączności i dotyczącej „ochrony prywatności klientów korzystających z usług sieci szerokopasmowych i innych usług telekomunikacyjnych”, co w praktyce oznacza odstąpienie od przepisów w sprawie ochrony prywatności w łączności szerokopasmowej, które wymagałyby od dostawców usług internetowych uzyskania od konsumentów jednoznacznej zgody przed sprzedaniem lub udostępnieniem agencjom reklamowym i innym przedsiębiorstwom danych o przeglądanych stronach internetowych i innych informacji o charakterze prywatnym; uważa to za kolejne zagrożenie dla gwarancji prywatności w Stanach Zjednoczonych;

**Kwestie dotyczące egzekwowania prawa i bezpieczeństwa narodowego**

20. uważa, że pojęcie „bezpieczeństwa narodowego” w mechanizmie Tarczy Prywatności nie jest szczegółowo wyjaśnione w sposób zapewniający, iż naruszenia ochrony danych mogą być skutecznie rozpatrywane przez sądy w celu zapewnienia zgodności z rygorystycznym testem pozwalającym stwierdzić, co jest niezbędne i proporcjonalne; apeluje w związku z tym o jasną definicję „bezpieczeństwa narodowego”;

21. zauważa, że z powodu postępu technologicznego i zmian wzorców komunikacyjnych, jak również stale zmieniającego się środowiska zagrożeń, wzrosła liczba celów przewidzianych w sekcji 702 ustawy o kontroli wywiadu;

22. ubolewa, że w związku z niedawnym ponownym zatwierdzeniem sekcji 702 ustawy o kontroli wywiadu USA nie skorzystały z tej okazji, aby uwzględnić w niej zabezpieczenia określone w dyrektywie politycznej Prezydenta nr 28; apeluje o dowody i prawnie wiążące zobowiązania zapewniające, że gromadzenie danych na mocy sekcji 702 ustawy o kontroli wywiadu nie jest nieograniczone oraz że dostęp do tych danych nie jest możliwy na podstawie uogólnionych przesłanek (hurtowe gromadzenie danych), co byłoby sprzeczne z Kartą praw podstawowych UE; przyjmuje do wiadomości wyjaśnienia Komisji zawarte w dokumencie roboczym służb Komisji, zgodnie z którymi inwigilacja prowadzona na podstawie sekcji 702 ustawy o kontroli wywiadu zawsze opiera się na kryteriach selekcyjnych i w związku z tym nie ma możliwości hurtowego gromadzenia danych; w związku z powyższym dołącza się do apeli formułowanych przez Grupę Roboczą Art. 29 domagającą się publikacji przez PCLOB zaktualizowanego sprawozdania dotyczącego definicji „celów”, „przydzielania zadań osobom dokonującym selekcji” i konkretnego procesu stosowania kryteriów selekcyjnych w kontekście programu UPSTREAM w celu wyjaśnienia i oceny, czy w tym kontekście ma miejsce hurtowy dostęp do danych osobowych; ubolewa nad faktem, że obywatele Unii są wykluczeni z dodatkowej ochrony przewidzianej na podstawie ponownego zatwierdzenia sekcji 702 ustawy o kontroli wywiadu; ubolewa, że ponownie zatwierdzona sekcja 702 zawiera kilka poprawek, które mają charakter czysto proceduralny i nie rozwiązują najbardziej palących problemów, przy czym kwestię tę poruszyła również Grupa Robocza Art. 29; wzywa Komisję do poważnego potraktowania zbliżającej się analizy sekcji 702 ustawy o kontroli wywiadu przeprowadzanej przez Grupę Roboczą Art. 29 i do podjęcia odpowiednich działań;

23. przyznaje, że ponowne zatwierdzenie sekcji 702 ustawy o kontroli wywiadu na kolejne sześć lat podaje w wątpliwość zgodność Tarczy Prywatności z prawem;

24. ponownie wyraża zaniepokojenie dekretem 12333, który umożliwia Narodowej Agencji Bezpieczeństwa (NSA) wymianę ogromnych ilości zgromadzonych prywatnych danych bez nakazów, orzeczeń sądów lub wydanych przez Kongres zezwoleń z 16 innymi agencjami, w tym z FBI, Agencją ds. Walki z Handlem Narkotykami i Departamentem Bezpieczeństwa Wewnętrznego; ubolewa nad brakiem jakiejkolwiek kontroli sądowej nad działaniami inwigilacyjnymi prowadzonymi na podstawie dekretu 12333;

25. podkreśla, że nadal istnieją przeszkody w stosowaniu środków odwoławczych przez osoby niebędące obywatelami ani rezydentami USA, które zostały poddane inwigilacji na mocy sekcji 702 ustawy o kontroli wywiadu lub dekretu 12333, wynikające z wymogów proceduralnych dotyczących wykazania interesu prawnego zgodnie z wykładnią stosowaną obecnie przez sądy w USA, które to przeszkody uniemożliwiają osobom niebędącym obywatelami ani rezydentami USA zaskarżanie w sądach w USA decyzji, które ich dotyczą;

26. wyraża zaniepokojenie skutkami dekretu 13768 w sprawie „zwiększenia bezpieczeństwa publicznego na terytorium Stanów Zjednoczonych” dla sądowych i administracyjnych środków ochrony prawnej dostępnych dla osób fizycznych w USA, ponieważ sposoby ochrony przewidziane w ustawie o ochronie prywatności nie mają już zastosowania do osób niebędących obywatelami ani rezydentami USA; przyjmuje do wiadomości stanowisko Komisji, zgodnie z którym ocena adekwatności ochrony danych nie opiera się na sposobach ochrony przewidzianych w ustawie o ochronie prywatności, a w związku z tym ten dekret nie wpływa na Tarczę Prywatności; uważa, że dekret 13768 dowodzi jednak, że władze wykonawcze USA mają zamiar cofnąć gwarancje ochrony udzielone wcześniej obywatelom Unii oraz zmienić zobowiązania na rzecz UE powzięte podczas prezydentury Baracka Obamy;

27. wyraża głębokie obawy dotyczące niedawnego przyjęcia ustawy wyjaśniającej zgodne z prawem transgraniczne wykorzystywanie danych, zwanej ustawą CLOUD (H.R. 4943), która poszerza zakres zdolności egzekwowania prawa w USA i poza granicami tego państwa do prowadzenia ukierunkowanych działań i uzyskiwania dostępu do danych osób w ramach operacji o charakterze transgranicznym bez stosowania instrumentów wzajemnej pomocy prawnej, które zapewniają odpowiednie zabezpieczenia i poszanowanie uprawnień organów sądowych krajów, w których znajdują się informacje; podkreśla, że ustawa CLOUD może nieść z sobą poważne konsekwencje dla UE, ponieważ przewiduje daleko idące rozwiązania i wywołuje potencjalny konflikt z unijnymi przepisami w dziedzinie ochrony danych;

28. uważa, że bardziej wyważonym rozwiązaniem byłoby wzmocnienie istniejącego międzynarodowego systemu traktatów o pomocy prawnej w celu sprzyjania współpracy międzynarodowej i sądowej; ponownie stwierdza, że zgodnie z art. 48 rozporządzenia (UE) 2016/679 (ogólnego rozporządzenia o ochronie danych) umowy o wzajemnej pomocy prawnej i inne umowy międzynarodowe stanowią preferowany mechanizm umożliwiający transgraniczny dostęp do danych osobowych;

29. ubolewa, że władze USA nie wywiązują się proaktywnie z powziętego zobowiązania do przedstawiania Komisji terminowych i kompleksowych informacji o wszelkich zmianach, które mogłyby być istotne z punktu widzenia Tarczy Prywatności, w tym nie powiadamiają Komisji o zmianach w amerykańskich ramach prawnych, na przykład o dekrecie prezydenta Donalda Trumpa nr 13768 w sprawie „zwiększenia bezpieczeństwa publicznego na terytorium Stanów Zjednoczonych” lub o uchyleniu przepisów dotyczących ochrony prywatności, które obowiązywały w odniesieniu do dostawców usług internetowych;

30. przypomina, że – jak wskazano w rezolucji z dnia 6 kwietnia 2017 r. – ani zasady Tarczy Prywatności, ani wyjaśnienia i zapewnienia w pismach administracji USA nie dowodzą istnienia skutecznych mechanizmów ochrony prawnej dla obywateli UE, których dane osobowe przekazywane są do organizacji amerykańskiej w oparciu o zasady Tarczy Prywatności, a następnie do których mają dostęp amerykańskie organy publiczne w celu ich przetwarzania na potrzeby egzekwowania prawa oraz w interesie publicznym, co podkreślił Trybunał Sprawiedliwości Unii Europejskiej w wyroku z dnia 6 października 2015 r. jako istotę prawa podstawowego, o którym mowa w art. 47 Karty praw podstawowych Unii Europejskiej;

**Wnioski**

31. wzywa Komisję do podjęcia wszystkich niezbędnych działań w celu zapewnienia, by Tarcza Prywatności była w pełni zgodna z rozporządzeniem (UE) 2016/679, którego stosowanie rozpoczyna się z dniem 25 maja 2018 r., oraz z Kartą praw podstawowych Unii Europejskiej, tak aby adekwatność ochrony danych nie prowadziła do luk lub przewagi komparatywnej dla przedsiębiorstw z USA;

32. wyraża ubolewanie, że Komisja i właściwe organy USA nie wznowiły dyskusji na temat ustaleń dotyczących Tarczy Prywatności i nie określiły żadnego planu działania mającego na celu jak najszybsze usunięcie wskazanych braków, o co apelowała Grupa Robocza Art. 29 w grudniowym sprawozdaniu dotyczącym wspólnego przeglądu; wzywa Komisję i właściwe organy USA, aby bez dalszej zwłoki przystąpiły do wskazanych wyżej działań;

33. przypomina, że ochrona prywatności i ochrona danych stanowią prawnie wiążące prawa podstawowe zapisane w traktatach, Karcie praw podstawowych Unii Europejskiej i europejskiej konwencji praw człowieka, a także w przepisach prawa i orzecznictwie; podkreśla, że prawa te muszą być stosowane w sposób, który niepotrzebnie nie utrudnia stosunków handlowych lub międzynarodowych, przy czym nie można uzależniać tych praw od interesów handlowych lub politycznych;

34. stoi na stanowisku, że obecne ustalenia dotyczące Tarczy Prywatności nie zapewniają odpowiedniego stopnia ochrony wymaganego przez prawo Unii w dziedzinie ochrony danych oraz Kartę praw podstawowych Unii Europejskiej zgodnie z wykładnią Trybunału Sprawiedliwości Unii Europejskiej;

35. uważa, że jeśli Stany Zjednoczone nie zapewnią pełnej zgodności przepisów do dnia 1 września 2018 r., będzie to oznaczać, że Komisja nie podjęła działań przewidzianych w art. 45 ust. 5 RODO; wzywa w związku z tym Komisję do zawieszenia Tarczy Prywatności do czasu, aż władze USA będą przestrzegać jej warunków;

36. zobowiązuje Komisję Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych do dalszego monitorowania rozwoju sytuacji w tym obszarze, w tym do monitorowania spraw wniesionych do Trybunału Sprawiedliwości, oraz do monitorowania działań następczych podjętych w związku z zaleceniami sformułowanymi w rezolucji;

37. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, rządom i parlamentom państw członkowskich oraz Radzie Europy.

1. Dz.U. L 119 z 4.5.2016, s. 1. [↑](#footnote-ref-1)
2. Dz.U. L 119 z 4.5.2016, s. 89. [↑](#footnote-ref-2)
3. EU:C:2015:650. [↑](#footnote-ref-3)
4. EU:C:2016:970. [↑](#footnote-ref-4)
5. Dz.U. L 207 z 1.8.2016, s. 1. [↑](#footnote-ref-5)
6. Dz.U. C 257 z 15.7.2016, s. 8. [↑](#footnote-ref-6)
7. <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf> [↑](#footnote-ref-7)
8. <http://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2016/wp236_en.pdf> [↑](#footnote-ref-8)
9. COM(2017)0611 z 18.10.2017 r. [↑](#footnote-ref-9)
10. SWD(2017)0344 z 18.10.2017 r. [↑](#footnote-ref-10)
11. Dokument WP 255 dostępny pod adresem <http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612621>. [↑](#footnote-ref-11)
12. Teksty przyjęte, P8\_TA(2017)0131. [↑](#footnote-ref-12)
13. <https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782> [↑](#footnote-ref-13)