C/2023/1073

15.12.2023

P9_TA(2023)0204

Adekwatność ochrony zapewnianej przez ramy ochrony danych UE–USA

Rezolucja Parlamentu Europejskiego z dnia 11 maja 2023 r. w sprawie adekwatności ochrony zapewnianej przez ramy ochrony danych UE–USA (2023/2501(RSP))

(C/2023/1073)

Parlament Europejski,

— uwzględniając Kartę praw podstawowych Unii Europejskiej (zwaną dalej „Kartą"), w szczególności jej art. 7, 8, 16, 47 i 52,

— uwzględniając wyrok Trybunału Sprawiedliwości Unii Europejskiej (TSUE) z 6 października 2015 r. w sprawie C-362/14 *Maximillian Schrems* przeciwko *Data Protection Commissioner* („Schrems I") ([1]),

— uwzględniając wyrok TSUE z 16 lipca 2020 r. w sprawie C-311/18 *Data Protection Commissioner* przeciwko *Facebook Ireland Limited i Maximillianowi Schremsowi* („Schrems II") ([2]),

— uwzględniając swoje dochodzenie w sprawie informacji, które ujawnił Edward Snowden, dotyczących masowej inwigilacji elektronicznej obywateli UE, w tym ustalenia zawarte w rezolucji z 12 marca 2014 r. w sprawie realizowanych przez NSA amerykańskich programów nadzoru, organów nadzoru w różnych państwach członkowskich oraz ich wpływu na prawa podstawowe obywateli UE oraz na współpracę transatlantycką w dziedzinie wymiaru sprawiedliwości i spraw wewnętrznych ([3]),

— uwzględniając swoją rezolucję z 26 maja 2016 r. w sprawie transatlantyckich przepływów danych ([4]),

— uwzględniając swoją rezolucję z 6 kwietnia 2017 r. w sprawie adekwatności ochrony zapewnianej przez tzw. Tarczę Prywatności UE-USA ([5]),

— uwzględniając swoją rezolucję z 5 lipca 2018 r. w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE–USA ([6]),

— uwzględniając swoją rezolucję z 20 maja 2021 r. w sprawie wyroku TSUE z 16 lipca 2020 r. – Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi („Schrems II") – sprawa C-311/18 ([7]),

— uwzględniając projekt decyzji wykonawczej Komisji na podstawie rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie odpowiedniego poziomu ochrony danych osobowych na mocy ram ochrony danych UE–USA,

— uwzględniając dekret Prezydenta Stanów Zjednoczonych nr 14086 z 7 października 2022 r. w sprawie wzmocnienia zabezpieczeń na potrzeby amerykańskiego rozpoznania radioelektronicznego,

— uwzględniając dekret Prezydenta Stanów Zjednoczonych nr 12333 z 4 grudnia 1981 r. w sprawie działalności wywiadowczej USA,

— uwzględniając rozporządzenie w sprawie sądu odwoławczego zajmującego się kwestiami ochrony danych wydane przez Prokuratora Generalnego Stanów Zjednoczonych,

---

([1]) Wyrok z 6 października 2015 r., *Maximillian Schrems* przeciwko *Data Protection Commissioner*, C-362/14, ECLI:EU:C:2015:650.
([2]) Wyrok z 16 lipca 2020 r., *Data Protection Commissioner* przeciwko *Facebook Ireland Limited i Maximillianowi Schremsowi*, C-311/18, ECLI:EU:C:2020:559.
([3]) Dz.U. C 378 z 9.11.2017, s. 104.
([4]) Dz.U. C 76 z 28.2.2018, s. 82.
([5]) Dz.U. C 298 z 23.8.2018, s. 73.
([6]) Dz.U. C 118 z 8.4.2020, s. 133.
([7]) Dz.U. C 15 z 12.1.2022, s. 176.

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 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) ([8]), w szczególności jego rozdział V,

— uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([9]),

— uwzględniając kryteria adekwatności ochrony przyjęte przez Grupę Roboczą Art. 29 (WP 254 rev.01), zatwierdzone przez Europejską Radę Ochrony Danych (EROD), uwzględniając zalecenia EROD 01/2020 dotyczące środków uzupełniających narzędzia przekazywania w celu zapewnienia zgodności z unijnym stopniem ochrony danych osobowych oraz zalecenia 02/2020 dotyczące niezbędnych gwarancji europejskich dla środków nadzoru,

— uwzględniając opinię Europejskiej Rady Ochrony Danych nr 5/2023 z 28 lutego 2023 r. dotyczącą projektu decyzji wykonawczej Komisji Europejskiej w sprawie odpowiedniej ochrony danych osobowych na mocy ram ochrony danych UE–USA,

— uwzględniając art. 132 ust. 2 Regulaminu,

A. mając na uwadze, że w wyroku w sprawie Schrems I TSUE unieważnił decyzję Komisji z dnia 26 lipca 2000 r., przyjętą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony przewidzianej przez zasady ochrony prywatności w ramach bezpiecznej przystani oraz przez odnoszące się do nich najczęściej zadawane pytania, wydane przez Departament Handlu USA ([10]), a także zwrócił uwagę, że nieograniczony dostęp organów wywiadowczych do treści łączności elektronicznej narusza istotę prawa podstawowego do poufności komunikacji przewidzianego w art. 7 Karty; mając na uwadze, że Trybunał zwrócił uwagę, że do celów decyzji stwierdzającej adekwatność ochrony państwo trzecie nie musi zapewniać poziomu identycznego z poziomem ochrony gwarantowanym w prawie UE, lecz poziom „merytorycznie równoważny", i można go zapewnić za pomocą różnych środków;

B. mając na uwadze, że w wyroku w sprawie Schrems II TSUE unieważnił decyzję wykonawczą Komisji (UE) 2016/1250 z dnia 12 lipca 2016 r., przyjętą na mocy dyrektywy 95/46/WE Parlamentu Europejskiego i Rady, w sprawie adekwatności ochrony zapewnianej przez Tarczę Prywatności UE-USA ([11]) i stwierdził, że nie zapewnia ona osobom niebędącym obywatelami USA wystarczających środków prawnych przeciwko masowej inwigilacji oraz że narusza to istotę prawa podstawowego do środka prawnego przewidzianego w art. 47 Karty;

C. mając na uwadze, że 7 października 2022 r. Prezydent Stanów Zjednoczonych podpisał dekret prezydencki nr 14086 w sprawie wzmocnienia zabezpieczeń na potrzeby amerykańskiego rozpoznania radioelektronicznego (dekret prezydencki 14086);

D. mając na uwadze, że 13 grudnia 2022 r. Komisja rozpoczęła proces przyjęcia decyzji w sprawie adekwatności ochrony w odniesieniu do ram ochrony danych UE–USA;

E. mając na uwadze, że badając poziom ochrony zapewniany przez państwo trzecie, Komisja jest zobowiązana do oceny treści przepisów obowiązujących w tym państwie, wynikających z jego prawa krajowego lub ze zobowiązań międzynarodowych, jak również praktyk mających zapewnić przestrzeganie tych przepisów; mając na uwadze, że jeżeli taka ochrona zostałaby uznana za niezadowalającą pod względem adekwatności i równoważności, Komisja powinna wstrzymać się od przyjęcia decyzji stwierdzającej adekwatność ochrony, ponieważ jest ona uzależniona od wdrożenia stosownych gwarancji; mając na uwadze, że Komisja jest zobowiązana zawiesić decyzję o adekwatności w przypadku ustania równoważności; mając na uwadze, że ogólne rozporządzenie o ochronie danych (RODO) wymaga, aby odpowiednia ocena była procesem ciągłym, uwzględniającym zmiany w obowiązujących przepisach i praktykach;

F. mając na uwadze, że możność transgranicznego przekazywania danych osobowych może być główną siłą napędową innowacji, wydajności i konkurencyjności gospodarczej, pod warunkiem zapewnienia odpowiednich zabezpieczeń; mając na uwadze, że przekazywanie tych danych powinno odbywać się z pełnym poszanowaniem prawa do ochrony danych osobowych oraz prawa do prywatności; mając na uwadze, że jednym z celów UE jest ochrona praw podstawowych zapisanych w Karcie;

([8]) Dz.U. L 119 z 4.5.2016, s. 1.
([9]) Dz.U. L 201 z 31.7.2002, s. 37.
([10]) Dz.U. L 215 z 25.8.2000, s. 7.
([11]) Dz.U. L 207 z 1.8.2016, s. 1.

G. mając na uwadze, że RODO ma zastosowanie do wszystkich przedsiębiorstw przetwarzających dane osobowe osób, których dotyczą dane, w UE, jeżeli przetwarzanie jest związane z oferowaniem takim osobom towarów lub usług w Unii lub z monitorowaniem ich zachowania, o ile zachowanie to ma miejsce na terenie Unii;

H. mając na uwadze, że masowa inwigilacja, tj. niewybiórcze gromadzenie danych bez żadnych zabezpieczeń służących ograniczeniu naruszeń prywatności osoby, prowadzona przez podmioty państwowe osłabia zaufanie europejskich obywateli i przedsiębiorstw do usług cyfrowych, a co za tym idzie, do gospodarki cyfrowej; mając na uwadze, że chociaż agencje amerykańskie nie mogą gromadzić danych masowych obywateli USA mieszkających w Stanach Zjednoczonych, zakaz ten nie ma zastosowania do obywateli UE; mając na uwadze, że masowa inwigilacja przez podmioty państwowe jest nielegalna i wpływa negatywnie na zaufanie obywateli europejskich i przedsiębiorstw unijnych do usług cyfrowych, a tym samym do gospodarki cyfrowej;

I. mając na uwadze, że administratorzy danych powinni zawsze ponosić odpowiedzialność za przestrzeganie obowiązków w dziedzinie ochrony danych, w tym za wykazanie zgodności w odniesieniu do każdego przetwarzania danych, niezależnie od charakteru, zakresu, kontekstu i celów przetwarzania oraz ryzyka dla osób, których dane dotyczą;

J. mając na uwadze, że w Stanach Zjednoczonych nie ma federalnych przepisów dotyczących prywatności i ochrony danych; mając na uwadze, że dekret prezydencki 14086 wprowadza definicje kluczowych pojęć ochrony danych, takich jak zasady konieczności i proporcjonalności, co stanowi istotny krok naprzód w porównaniu z poprzednimi mechanizmami przekazywania; mając na uwadze, że sposób interpretacji tych zasad wymaga bacznego monitorowania; mając na uwadze, że kompleksowa ocena, jak te zasady są stosowane w porządku prawnym USA, może nie być możliwa ze względu na brak przejrzystości procedur sądu odwoławczego zajmującego się kwestiami ochrony danych (DPRC);

1. przypomina, że poszanowanie życia prywatnego i rodzinnego oraz ochrona danych osobowych stanowią możliwe do wyegzekwowania na drodze prawnej prawa podstawowe zapisane w traktatach, Karcie i europejskiej konwencji praw człowieka, a także w przepisach prawa i orzecznictwie; podkreśla, że decyzje stwierdzające adekwatność ochrony podejmowane na podstawie RODO są decyzjami prawnymi, a nie politycznymi, oraz że praw do prywatności i ochrony danych nie można zrównoważyć z interesami handlowymi lub politycznymi, lecz jedynie z innymi prawami podstawowymi;

2. zauważa, że w dekrecie prezydenckim 14086 podjęto starania, aby ograniczyć amerykańskie rozpoznanie radioelektroniczne przez to, że zastosowano zasady proporcjonalności i konieczności do ram prawnych USA dotyczących rozpoznania radioelektronicznego oraz ustalono wykaz uzasadnionych celów takich działań; zauważa, że zasady te byłyby wiążące dla całej Wspólnoty Wywiadów USA oraz że osoby, których dane dotyczą, mogłyby się na nie powoływać w ramach procedury przewidzianej w dekrecie prezydenckim 14086; podkreśla, że ten dekret prezydencki przewiduje znaczne usprawnienia mające zagwarantować, że zasady te będą zasadniczo równoważne zasadom w prawie UE; zwraca jednak uwagę, że zasady te są od dawna kluczowymi elementami unijnego systemu ochrony danych oraz że ich merytoryczne definicje w dekrecie prezydenckim 14086 nie są zgodne z ich definicją zawartą w prawie UE i z wykładnią TSUE; zwraca ponadto uwagę, że do celów ram ochrony danych UE–USA zasady te byłyby interpretowane wyłącznie w świetle prawa i tradycji prawnych USA, a nie prawa i tradycji prawnych UE; zauważa, że w dekrecie prezydenckim 14086 wymieniono 12 uzasadnionych celów, które można realizować przy gromadzeniu danych podczas rozpoznania radioelektronicznego, oraz pięć celów, w przypadku których gromadzenie danych podczas rozpoznania radioelektronicznego jest zakazane; zauważa, że Prezydent USA może zmienić i rozszerzyć wykaz uzasadnionych celów w zakresie bezpieczeństwa narodowego bez obowiązku podawania odpowiednich aktualizacji do wiadomości publicznej ani informowania o tym UE; zwraca uwagę, że w dekrecie prezydenckim 14086 wymaga się, aby rozpoznanie radioelektroniczne prowadzono w sposób konieczny i proporcjonalny do „zweryfikowanego priorytetu wywiadowczego", co wydaje się być szeroką wykładnią tych koncepcji; podkreśla, że kompleksowa ocena zasad proporcjonalności i konieczności w kontekście dekretu prezydenckiego 14086 wymagałaby ich wdrożenia i stosowania w strategiach politycznych i procedurach amerykańskich agencji wywiadowczych; wyraża jednak zaniepokojenie, że nie ma wymogu, aby analitycy przeprowadzali ocenę proporcjonalności każdej decyzji wywiadowczej;

3. zauważa, że w dekrecie prezydenckim 14086 dopuszcza się w niektórych przypadkach masowe gromadzenie danych za pomocą rozpoznania radioelektronicznego, w tym treści komunikacji; zauważa jednocześnie, że dekret prezydencki 14086 przewiduje, iż ukierunkowane gromadzenie danych powinno mieć pierwszeństwo przed masowym gromadzeniem; przypomina, że chociaż dekret prezydencki 14086 zawiera kilka zabezpieczeń w przypadku masowego gromadzenia, nie przewiduje niezależnego uprzedniego zezwolenia na masowe gromadzenie; nie przewiduje go również dekret prezydencki 12333; przypomina, że w wyroku w sprawie Schrems II TSUE wyjaśnił, że inwigilacja prowadzona przez USA nie jest zgodna z prawem UE, ponieważ nie wymaga spełnienia „obiektywnego kryterium" „umożliwiającego uzasadnienie"

ingerencji rządu w prywatność; zwraca uwagę, że podważa to zasadność celów jako zabezpieczenia służącego ograniczeniu działalności wywiadowczej USA; przypomina, że po przyjęciu dyrektywy prezydenckiej nr 28 (PPD-28), która stanowiła podstawę decyzji stwierdzającej adekwatność ochrony zapewnianej przez Tarczę Prywatności, Rada Nadzoru nad Prywatnością i Wolnościami Obywatelskimi (PCLOB) wydała sprawozdanie z przeglądu ([12]) i stwierdziła, że w PPD-28 zasadniczo utrzymano dotychczasowe praktyki Wspólnoty Wywiadów; jest przekonany, że PPD-28 nie spowoduje, że władze USA zaprzestaną elektronicznej masowej inwigilacji obywateli UE;

4. podziela obawy EROD, że dekret prezydencki 14086 nie zapewnia wystarczających zabezpieczeń w przypadku masowego gromadzenia danych, a mianowicie nie przewiduje niezależnego uprzedniego zezwolenia, jasnych i rygorystycznych przepisów dotyczących zatrzymywania danych, „tymczasowego" masowego gromadzenia danych ani bardziej rygorystycznych zabezpieczeń dotyczących rozpowszechniania danych gromadzonych masowo; wskazuje zwłaszcza na szczególną obawę, że bez dalszych ograniczeń dotyczących udostępniania informacji władzom amerykańskim organy ścigania będą mogły uzyskać wgląd w dane, do których w innym przypadku miałyby zakaz dostępu; przypomina, że wtórne przekazywanie danych w praktyce zwielokrotnia ryzyko dla ochrony danych; zauważa, że EROD zaapelowała o włączenie prawnie wiążącego obowiązku przeanalizowania i ustalenia, czy państwo trzecie oferuje akceptowalny minimalny poziom zabezpieczeń;

5. zwraca uwagę, że dekretu prezydenckiego 14086 nie stosuje się do danych, do których organy publiczne uzyskują dostęp za pomocą innych środków, na przykład amerykańskiej ustawy CLOUD lub ustawy PATRIOT, zakupów danych komercyjnych lub dobrowolnych umów o udostępnianiu danych;

6. zwraca uwagę, że podstawowym problemem jest inwigilacja osób spoza USA na mocy prawa amerykańskiego oraz brak możliwości dochodzenia roszczeń w tym zakresie przez obywateli europejskich; domaga się, aby obywatele UE mieli takie same prawa i przywileje, jakie przysługują obywatelom USA, jeśli chodzi o działalność amerykańskiej Wspólnoty Wywiadów i dostęp do sądów w USA;

7. zauważa, że według wykładni USA „rozpoznanie radioelektroniczne" obejmuje wszystkie metody dostępu do danych przewidziane w ustawie o kontroli wywiadu (FISA), w tym danych pochodzących od dostawców „zdalnych usług obliczeniowych", zgodnie ze zmianami do FISA (§ 1881a) z 2008 r.; wzywa Komisję, aby w przyszłych negocjacjach wyjaśniła definicję i zakres pojęcia „rozpoznanie radioelektroniczne" używanego w dekrecie prezydenckim 14086; przypomina, że zgodnie z sekcją 702 FISA administracja Stanów Zjednoczonych nadal utrzymuje, że ma prawo obierać za cel osoby niebędące obywatelami USA za granicą, aby uzyskać zagraniczne informacje wywiadowcze w szerokim rozumieniu tego pojęcia;

8. wskazuje, że stworzono nowy mechanizm dochodzenia roszczeń umożliwiający osobom z UE, których dane dotyczą, składanie skarg; jednocześnie podkreśla, że decyzje DPRC byłyby niejawne i nie byłyby podawane do wiadomości publicznej ani udostępniane skarżącemu, którego by jedynie informowano, że w procedurze odwoławczej nie stwierdzono żadnych naruszeń objętych dochodzeniem lub że DPRC wydał postanowienie wymagające podjęcia odpowiednich działań – stanowi to naruszenie prawa skarżących do dostępu do ich danych lub ich sprostowania; wyraża zaniepokojenie, że oznacza to, iż osoba wnosząca sprawę nie miałaby możliwości uzyskania informacji o jej merytorycznym rozstrzygnięciu, a decyzja byłaby ostateczna; zauważa, że proponowana procedura odwoławcza nie przewiduje możliwości odwołania się do sądu federalnego, a zatem między innymi nie daje skarżącemu żadnej możliwości dochodzenia odszkodowania; wzywa Komisję, aby kontynuowała negocjacje ze Stanami Zjednoczonymi w celu wprowadzenia niezbędnych zmian, które pozwoliłyby rozwiązać te problemy;

9. zauważa, że dekret prezydencki 14086 wprowadza kilka gwarancji, aby zapewnić niezależność sędziów DPRC, jak uznała EROD w swojej opinii; zwraca uwagę, że DPRC należy do władzy wykonawczej, a nie sądowniczej, i jego sędziowie są powoływani na czteroletnią kadencję; podkreśla, że Prezydent USA może uchylać decyzje DPRC, nawet w tajemnicy; zwraca uwagę, że choć nowy mechanizm dochodzenia roszczeń nie pozwala Prokuratorowi Generalnemu USA odwoływać i nadzorować sędziów DPRC, nie wpływa jednak na odpowiednie uprawnienia Prezydenta USA; podkreśla, że dopóki Prezydent USA może usunąć sędziów DPRC w trakcie ich kadencji, nie można zagwarantować niezależności tych sędziów; zauważa, że w przypadku przyjęcia Komisja będzie musiała ściśle monitorować stosowanie tych gwarancji, aby zapewnić faktyczną niezależność; wskazuje, że skarżący byłby reprezentowany przez „specjalnego obrońcę" wyznaczonego przez DPRC i niepodlegającego wymogowi niezależności; wzywa Komisję, aby w razie przyjęcia decyzji stwierdzającej adekwatność ochrony dopilnowała wprowadzenia wymogu niezależności; stwierdza, że w obecnej formie DPRC nie spełnia standardów niezależności i bezstronności określonych w art. 47 Karty; zauważa, że chociaż PCLOB ma przeprowadzać niezależny przegląd funkcjonowania nowego procesu dochodzenia roszczeń, zakres tego przeglądu byłby ograniczony;

([12]) PCLOB, *Report to the President on the Implementation of Presidential Directive 28: Signals Intelligence Activities* [Sprawozdanie dla Prezydenta w sprawie wdrożenia dyrektywy prezydenckiej nr 28: Działania w zakresie rozpoznania radioelektronicznego].

10. zauważa, że Stany Zjednoczone przewidziały nowy mechanizm środków zaradczych w sprawach związanych z dostępem organów publicznych do danych, lecz nadal pozostają wątpliwości co do skuteczności środków zaradczych dostępnych w sprawach handlowych, niezmienionych na mocy decyzji stwierdzającej adekwatność; zauważa, że mechanizmy służące rozwiązaniu tych problemów w dużej mierze pozostają w gestii przedsiębiorstw, które mogą wybrać alternatywne środki zaradcze, takie jak mechanizmy rozstrzygania sporów lub skorzystanie z programów ochrony prywatności przedsiębiorstw; wzywa Komisję, aby w razie przyjęcia decyzji stwierdzającej adekwatność uważnie analizowała skuteczność tych mechanizmów dochodzenia roszczeń;

11. zauważa, że europejskie przedsiębiorstwa potrzebują pewności prawa i zasługują na nią; podkreśla, że seria mechanizmów przekazywania danych, uchylanych następnie przez TSUE, spowodowała dodatkowe koszty dla europejskich przedsiębiorstw; dostrzega w związku z tym, że trzeba zapewnić pewność prawa i uniknąć sytuacji, w której przedsiębiorstwa muszą stale dostosowywać się do nowych rozwiązań prawnych, co może być szczególnie uciążliwe dla mikroprzedsiębiorstw oraz małych i średnich przedsiębiorstw; wyraża zaniepokojenie, że decyzja stwierdzająca adekwatność ochrony, jeśli zostanie przyjęta, mogłaby zostać unieważniona przez TSUE (podobnie jak wcześniejsze decyzje), co prowadziłoby do ciągłego braku pewności prawa, dalszych kosztów i zakłóceń dla europejskich obywateli i przedsiębiorstw;

12. zwraca uwagę, że w przeciwieństwie do wszystkich innych państw trzecich, które otrzymały decyzję stwierdzającą adekwatność ochrony na podstawie RODO, w Stanach Zjednoczonych wciąż nie ma federalnych przepisów o ochronie danych; zwraca uwagę, że stosowanie dekretu prezydenckiego 14086 nie jest jasne, precyzyjne ani przewidywalne, a Prezydent USA może go zmienić lub uchylić w dowolnym momencie, a także ma prawo wydawać tajne dekrety prezydenckie; zauważa, że przegląd ustalenia stwierdzającego adekwatność ma nastąpić po roku od daty powiadomienia państw członkowskich o decyzji stwierdzającej adekwatność ochrony, a następnie taki przegląd ma być przeprowadzany przynajmniej raz na cztery lata; wzywa Komisję, aby w razie przyjęcia jakiejkolwiek przyszłej decyzji stwierdzającej adekwatność ochrony przeprowadzała kolejne przeglądy przynajmniej raz na trzy lata, zgodnie z postulatem zawartym w opinii EROD; wyraża zaniepokojenie brakiem klauzuli wygaśnięcia przewidującej, że decyzja automatycznie traci ważność cztery lata po jej wejściu w życie, po czym Komisja musiałaby wydać nowe postanowienie; wyraża zaniepokojenie, że brak klauzuli wygaśnięcia w tej decyzji stwierdzającej adekwatność ochrony oznacza łagodniejsze podejście do Stanów Zjednoczonych, mimo że amerykańskie ramy ochrony prywatności opierają się na dekrecie prezydenckim, który pozwala na tajne zmiany i który można zmieniać bez zgody Kongresu i bez informowania partnerów z UE; w związku z tym wzywa Komisję do wprowadzenia takiej klauzuli;

13. podziela obawy wyrażane przez EROD dotyczące praw osób, których dane dotyczą, braku kluczowych definicji i szczegółowych przepisów dotyczących zautomatyzowanego podejmowania decyzji i profilowania, braku jasności co do stosowania zasad ram ochrony danych do podmiotów przetwarzających dane oraz konieczności unikania wtórnego przekazywania danych, które osłabia poziom ochrony;

14. podkreśla, że decyzje stwierdzające adekwatność ochrony muszą zawierać jasne i rygorystyczne mechanizmy monitorowania i przeglądu, aby zapewnić aktualność decyzji albo ich odwołanie lub zmianę w razie potrzeby, a także zagwarantować podstawowe prawo obywateli UE do ochrony danych w każdym momencie; podkreśla, że każda przyszła decyzja stwierdzająca adekwatność ochrony podlegałaby stałemu przeglądowi, z uwzględnieniem zmian prawnych i praktycznych w USA;

Wnioski

15. przypomina, że w rezolucji z 20 maja 2021 r. Parlament wezwał Komisję, aby nie przyjmowała nowej decyzji stwierdzającej adekwatność ochrony w odniesieniu do Stanów Zjednoczonych, chyba że wprowadzone zostaną istotne reformy, w szczególności do celów bezpieczeństwa narodowego i wywiadu; nie uważa dekretu prezydenckiego 14086 za wystarczająco istotny; ponownie stwierdza, że Komisja nie powinna pozostawiać zadania ochrony podstawowych praw obywateli UE Trybunałowi Sprawiedliwości Unii Europejskiej w następstwie skarg poszczególnych obywateli;

16. przypomina, że Komisja musi ocenić adekwatność ochrony w państwie trzecim na podstawie obowiązujących przepisów i praktyk nie tylko pod względem merytorycznym, ale również w praktyce, jak określono w sprawach Schrems I i Schrems II oraz RODO (motyw 104);

17. zauważa, że ramy ochrony danych ustanowione przez Departament Handlu USA nie zostały wystarczająco zmienione w porównaniu z zasadami Tarczy Prywatności tak, aby zapewnić ochronę równoważną co do zasady z ochroną przewidzianą w RODO;

18. zauważa, że chociaż Stany Zjednoczone podejmują istotne zobowiązanie do poprawy dostępu do środków ochrony prawnej i przepisów dotyczących przetwarzania danych przez organy publiczne, Wspólnota Wywiadu USA musi do października 2023 r. zaktualizować swoją politykę i praktyki zgodnie z dekretem prezydenckim 14086, oraz że rzecznik generalny USA nie uznał jeszcze UE i jej państw członkowskich za państwa kwalifikujące się do uzyskania dostępu do środków odwoławczych przewidzianych w DPRC; podkreśla, że oznacza to, iż Komisja nie była w stanie ocenić

skuteczności proponowanych środków zaradczych i proponowanych środków w zakresie dostępu do danych „w praktyce"; stwierdza w związku z tym, że Komisja może przystąpić do kolejnego etapu decyzji stwierdzającej adekwatność ochrony dopiero po tym, jak Stany Zjednoczone dotrzymają terminów i osiągną cele pośrednie, aby zapewnić wykonanie zobowiązań w praktyce;

19. stwierdza, że ramy ochrony danych UE–USA nie zapewniają zasadniczej równoważności poziomu ochrony; wzywa Komisję, aby kontynuowała negocjacje ze swoimi amerykańskimi odpowiednikami w celu stworzenia mechanizmu, który zapewniłby taką równoważność i odpowiedni poziom ochrony wymagany przez unijne prawo o ochronie danych i Kartę zgodnie z wykładnią TSUE; wzywa Komisję, aby nie przyjmowała ustalenia stwierdzającego adekwatność ochrony do czasu pełnego wdrożenia wszystkich zaleceń zawartych w niniejszej rezolucji i opinii EROD;

20. wzywa Komisję, aby działała w interesie unijnych przedsiębiorstw i obywateli i dopilnowała, żeby proponowane ramy tworzyły solidną, wystarczającą i zorientowaną na przyszłość podstawę prawną przekazywania danych między UE a USA; spodziewa się, że każda decyzja stwierdzająca adekwatność ochrony, jeżeli zostanie przyjęta, będzie ponownie zaskarżona przed TSUE; zwraca uwagę na odpowiedzialność Komisji za brak ochrony praw obywateli UE w sytuacji, gdy TSUE ponownie unieważni decyzję stwierdzającą adekwatność ochrony;

o

o o

21. zobowiązuje swoją przewodniczącą do przekazania niniejszej rezolucji Radzie, Komisji oraz Prezydentowi i Kongresowi Stanów Zjednoczonych Ameryki.