Czwartek, 13 grudnia 2018 r.

P8_TA(2018)0529

Dostateczna ochrona danych osobowych udzielana przez Japonię

Rezolucja Parlamentu Europejskiego z dnia 13 grudnia 2018 r. w sprawie adekwatności ochrony danych osobowych zapewnianej przez Japonię (2018/2979(RSP))

(2020/C 388/16)

Parlament Europejski,

— uwzględniając Traktat o Unii Europejskiej, Traktat o funkcjonowaniu Unii Europejskiej oraz art. 6, 7, 8, 11, 16, 47 i 52 Karty praw podstawowych Unii Europejskiej,

— 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) [RODO] ([1]) oraz inne odpowiednie przepisy europejskie o ochronie danych,

— uwzględniając wyrok Trybunału Sprawiedliwości UE z 6 października 2015 r. w sprawie C-362/14 (Maximillian Schrems przeciwko Data Protection Commissioner) ([2]),

— uwzględniając wyrok Trybunału Sprawiedliwości UE z 21 grudnia 2016 r. w sprawach połączonych 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.) ([3]),

— uwzględniając swoją rezolucję z 12 grudnia 2017 r. zatytułowaną „W kierunku strategii w zakresie handlu elektronicznego” ([4]),

— uwzględniając dokument Grupy Roboczej Art. 29 zatytułowany „Odpowiedni stopień ochrony przekazywanych danych osobowych” z 6 lutego 2018 r. ([5]), w którym na podstawie RODO przedstawiono wytyczne dla Komisji i Europejskiej Rady Ochrony Danych (EROD) dotyczące oceny stopnia ochrony danych w państwach trzecich i organizacjach międzynarodowych,

— uwzględniając opinię Europejskiej Rady Ochrony Danych z 5 grudnia 2018 r. w sprawie projektu decyzji stwierdzającej równoważny poziom ochrony danych osobowych w UE i Japonii,

— uwzględniając projekt decyzji wykonawczej Komisji na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie odpowiedniego stopnia ochrony danych osobowych zapewnianej przez Japonię (COM(2018) XXXX),

— uwzględniając ustalenia z wizyty delegacji ad hoc Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w Japonii, zorganizowanej w październiku 2017 r. w związku z negocjacjami w sprawie odpowiedniego stopnia ochrony, by spotkać się z odpowiednimi organami japońskimi i zainteresowanymi stronami i omówić zasadnicze elementy do rozważenia przez Komisję Europejską przy podejmowaniu decyzji w sprawie odpowiedniego stopnia ochrony,

— uwzględniając art. 123 ust. 2 Regulaminu,

A. mając na uwadze, że RODO stosuje się od 25 maja 2018 r.; mając na uwadze, że w art. 45 ust. 2 RODO określono elementy, które powinna uwzględnić Komisja, oceniając stopień ochrony w państwie trzecim lub organizacji międzynarodowej;

B. mając na uwadze, że Komisja musi uwzględnić w szczególności praworządność, poszanowanie praw człowieka i podstawowych wolności, odpowiednie ustawodawstwo – zarówno ogólne, jak i sektorowe – w tym w dziedzinie bezpieczeństwa publicznego, obrony, bezpieczeństwa narodowego i prawa karnego oraz dostępu organów publicznych do danych osobowych, istnienie i skuteczne działanie co najmniej jednego niezależnego organu nadzorczego oraz międzynarodowe zobowiązania podjęte przez dane państwo trzecie lub daną organizację międzynarodową;

([1]) Dz.U. L 119 z 4.5.2016, s. 1.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2016:970.
([4]) Dz.U. C 369 z 11.10.2018, s. 22.
([5]) http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=614108; zatwierdzony przez EROD na pierwszym posiedzeniu plenarnym.

C. mając na uwadze, że Trybunał Sprawiedliwości UE w wyroku z 6 października 2015 r. w sprawie C-362/14 (Maximillian Schrems przeciwko Data Protection Commissioner) wyjaśnił, że odpowiedni stopień ochrony w państwie trzecim należy rozumieć jako poziom ochrony „merytorycznie równoważny" poziomowi gwarantowanemu w Unii Europejskiej na mocy dyrektywy 95/46/WE odczytywanej w świetle postanowień Karty;

D. mając na uwadze, że Japonia należy do kluczowych partnerów handlowych UE oraz że UE niedawno zawarła z Japonią umowę o partnerstwie gospodarczym, w której zapisano wspólne wartości i zasady przy zachowaniu ochrony spraw szczególnie istotnych dla obu stron; mając na uwadze, że powszechne uznanie praw podstawowych, w tym ochrony prywatności i ochrony danych, to istotna podstawa decyzji w sprawie odpowiedniej ochrony danych osobowych, która będzie podstawą prawną przekazywania danych osobowych z UE do Japonii;

E. mając na uwadze, że delegację ad hoc Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w Japonii poinformowano, że organy japońskie i tamtejsze zainteresowane strony są zainteresowane nie tylko stosowaniem nowych przepisów RODO, ale również opracowaniem solidnego mechanizmu przekazywania danych osobowych na wysokim poziomie między UE a Japonią, spełniającego określone w unijnych przepisach warunki dotyczące poziomu ochrony uznawanego za merytorycznie równoważny z poziomem przewidzianym w przepisach UE dotyczących ochrony danych;

F. mając na uwadze, że wobec stale postępującej cyfryzacji światowej gospodarki przekazywanie danych osobowych między UE a Japonią w celach handlowych to ważny element stosunków między obiema stronami; 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 zapisana w Karcie praw podstawowych Unii Europejskiej;

G. mając na uwadze, że w styczniu 2017 r. UE i Japonia rozpoczęły dyskusje dotyczące ułatwienia przekazywania danych osobowych w celach handlowych na podstawie uzgodnionego po raz pierwszy „wzajemnego uznania systemów ochrony danych za równoważne"; mając na uwadze, że w rezolucji z 12 grudnia 2017 r. zatytułowanej „W kierunku strategii w zakresie handlu cyfrowego" Parlament jednoznacznie „uzna[ł], że decyzje stwierdzające odpowiedni stopień ochrony […] są podstawowym mechanizmem zabezpieczania przekazywania danych osobowych z UE do państwa trzeciego";

H. mając na uwadze, że decyzja stwierdzająca odpowiedni stopień ochrony w odniesieniu do przekazywania danych osobowych do Japonii byłaby pierwszą taką decyzją przyjętą zgodnie z nowymi, bardziej rygorystycznymi przepisami RODO;

I. mając na uwadze, że Japonia niedawno zmodernizowała i udoskonaliła swoje przepisy dotyczące ochrony danych, by dostosować je do norm międzynarodowych, zwłaszcza do zabezpieczeń i praw indywidualnych przewidzianych w nowych europejskich przepisach dotyczących ochrony danych; mając na uwadze, że japońskie przepisy o ochronie danych opierają się na kilku filarach, a centralnym aktem prawnym w tej dziedzinie jest ustawa o ochronie informacji osobowych;

J. mając na uwadze, że Rada Ministrów Japonii wydała 12 czerwca 2018 r. zarządzenie, w którym przekazała Komisji Ochrony Informacji Osobowych jako organowi właściwemu do wdrażania ustawy o ochronie informacji osobowych „uprawnienie do podejmowania działań niezbędnych do niwelowania różnic między systemami i operacjami Japonii i zainteresowanego państwa obcego na podstawie art. 6 ustawy w celu zapewnienia właściwego postępowania z informacjami osobowymi otrzymanymi z tego państwa"; mając na uwadze, że według tej decyzji obejmuje to prawo Komisji Ochrony Informacji Osobowych do wprowadzania zwiększonej ochrony przez przyjęcie bardziej rygorystycznych zasad uzupełniających przepisy ustawy o ochronie informacji osobowych i zarządzenia Rady Ministrów oraz wykraczających poza nie; mając na uwadze, że zgodnie z tą decyzją takie bardziej rygorystyczne zasady będą wiążące dla japońskich podmiotów gospodarczych i mogą być od nich egzekwowane;

K. mając na uwadze, że projektowi decyzji wykonawczej Komisji w sprawie odpowiedniego stopnia ochrony danych osobowych zapewnianej przez Japonię towarzyszą, jako załącznik I, Zasady uzupełniające przyjęte 15 czerwca 2018 r. przez Komisję Ochrony Informacji Osobowych na podstawie art. 6 ustawy o ochronie informacji osobowych, jednoznacznie zezwalającej Komisji Ochrony Informacji Osobowych na przyjmowanie bardziej rygorystycznych zasad, w tym w celu ułatwienia międzynarodowego transferu danych; mając jednak na uwadze, że te zasady uzupełniające nie są jeszcze dostępne publicznie;

L. mając na uwadze, że celem zasad uzupełniających ma być zniwelowanie istotnych różnic między japońskimi a unijnymi przepisami o ochronie danych, by zapewnić właściwe postępowanie z informacjami osobowymi otrzymywanymi z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, zwłaszcza w odniesieniu do informacji osobowych wymagających szczególnej uwagi („dane wrażliwe"), zatrzymanych danych osobowych, określenia celu wykorzystywania, ograniczenia ze względu na cel wykorzystywania, ograniczenia udostępniania osobom trzecim w obcym kraju oraz informacji przetwarzanych anonimowo;

M. mając na uwadze, że zasady uzupełniające będą prawnie wiążące dla każdego podmiotu gospodarczego przetwarzającego informacje osobowe, który otrzymuje dane osobowe przekazane z UE na podstawie decyzji stwierdzającej odpowiedni stopień ochrony, a zatem jest zobowiązany do przestrzegania tych zasad oraz wszelkich powiązanych praw i obowiązków, a ponadto zasady te będą egzekwowane przez Komisję Ochrony Informacji Osobowych i japońskie sądy;;

N. mając na uwadze, że w celu zapewnienia merytorycznie równoważnego poziomu ochrony danych osobowych przekazywanych z UE do Japonii w zasadach dodatkowych wprowadzono dodatkowe zabezpieczenia mające zastosowanie na podstawie surowszych warunków lub ograniczeń dotyczących przetwarzania danych osobowych z UE, na przykład w przypadku informacji osobowych wymagających szczególnej uwagi, wtórnego przekazywania, danych anonimowych i ograniczenia celu;

O. mając na uwadze, że w japońskich przepisach o ochronie danych rozróżnia się „dane osobowe" i „informacje osobowe", a w niektórych przypadkach wprowadza się odniesienie do szczególnej kategorii danych osobowych, mianowicie „zatrzymanych danych osobowych";

P. mając na uwadze, że zgodnie z art. 2 ust. 1 ustawy o ochronie informacji osobowych pojęcie „informacje osobowe" obejmuje wszelkie informacje dotyczące żywej osoby i umożliwiające jej identyfikację; mając na uwadze, że w definicji tej rozróżnia się dwie kategorie informacji osobowych: (i) indywidualne kody identyfikacyjne oraz (ii) inne informacje osobowe umożliwiające zidentyfikowanie konkretnej osoby; mając na uwadze, że ta druga kategoria obejmuje informacje, które same w sobie nie umożliwiają identyfikacji, ale po „łatwym zestawieniu" z innymi informacjami mogą umożliwić identyfikację konkretnej osoby;

Q. mając na uwadze, że zgodnie z art. 2 ust. 4 ustawy o ochronie informacji osobowych pojęcie „dane osobowe" oznacza informacje osobowe stanowiące bazę danych osobowych itp.; mając na uwadze, że art. 2 ust. 1 tej ustawy precyzuje, że informacje zawarte w takich bazach danych są systematycznie porządkowane, co przypomina pojęcie zbioru danych z art. 2 ust. 1 RODO; mając na uwadze, że zgodnie z art. 4 pkt 1 RODO „dane osobowe" oznaczają informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej; mając na uwadze, że możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy bądź jeden lub kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej; mając na uwadze, że aby stwierdzić, czy dana osoba fizyczna jest możliwa do zidentyfikowania, należy wziąć pod uwagę wszelkie metody (w tym wyodrębnienie wpisów dotyczących tej samej osoby), które mogą być z uzasadnionym prawdopodobieństwem wykorzystane przez administratora lub inną osobę do bezpośredniego lub pośredniego zidentyfikowania osoby fizycznej;

R. mając na uwadze, że zgodnie z art. 2 ust. 7 ustawy o ochronie informacji osobowych „zatrzymane dane osobowe" oznaczają dane osobowe, które podmiot gospodarczy zajmujący się przetwarzaniem informacji osobowych ma prawo ujawniać, poprawiać, uzupełniać lub usuwać, zaprzestać wykorzystywać, skasować albo zaprzestać dostarczać osobie trzeciej, a nie są to dane wskazane w zarządzeniu Rady Ministrów jako mogące zaszkodzić interesom publicznym lub innym interesom, jeśli ich obecność lub brak zostaną ujawnione, ani dane, które mają być usunięte w terminie nie dłuższym niż rok, określonym w zarządzeniu Rady Ministrów; mając na uwadze, że w zasadach uzupełniających zrównano pojęcie „zatrzymanych danych osobowych" z pojęciem „danych osobowych", by zagwarantować, że niektóre dotyczące ich ograniczenia praw indywidualnych nie będą miały zastosowania do danych przekazywanych z UE;

S. mając na uwadze, że z zakresu japońskiej ustawy o ochronie danych będącej przedmiotem projektu decyzji wykonawczej wyłączono przetwarzanie danych osobowych przez niektóre sektory do konkretnych celów; mając na uwadze, że projekt decyzji wykonawczej nie miałby zastosowania do przekazywania danych osobowych z UE odbiorcy objętemu którymkolwiek z tych wyjątków przewidzianych w japońskiej ustawie o ochronie danych;

T. mając na uwadze, że w odniesieniu do wtórnego przekazywania unijnych danych osobowych z Japonii do państwa trzeciego w projekcie decyzji wykonawczej wyłączono stosowanie instrumentów przekazywania nietworzących wiążącego stosunku między japońskim podmiotem przekazującym dane a przyjmującym dane podmiotem z państwa trzeciego i niegwarantujących wymaganego poziomu ochrony; mając na uwadze, że dotyczy to na przykład systemu transgranicznych zasad ochrony prywatności organizacji Współpraca Gospodarcza Azji i Pacyfiku (APEC CBPR), w którym Japonia uczestniczy, ponieważ w tym systemie ochrona nie wynika z dwustronnej umowy wiążącej eksportera z importerem, a jej poziom jest wyraźnie niższy niż poziom gwarantowany przez połączenie ustawy o ochronie informacji osobowych i zasad uzupełniających;

U. mając na uwadze, że w opinii z 5 grudnia 2018 r. Europejska Rada Ochrony Danych oceniła, na podstawie dokumentacji udostępnionej przez Komisję, czy japońskie przepisy o ochronie danych zapewniają wystarczające gwarancje odpowiedniego poziomu ochrony danych osób fizycznych; mając na uwadze, że Europejska Rada Ochrony Danych z zadowoleniem przyjęła starania Komisji Europejskiej oraz japońskiej Komisji Ochrony Informacji Osobowych o większe zbliżenie japońskich i europejskich przepisów w celu ułatwienia przekazywania danych osobowych; mając na uwadze, że zdaniem Europejskiej Rady Ochrony Danych wprowadzone ulepszenia w postaci zasad uzupełniających, mające niwelować niektóre różnice między przepisami obu stron, są bardzo ważne i zostały dobrze przyjęte; mając na uwadze, że Rada odnotowała pewne utrzymujące się obawy, np. o to, czy dane osobowe przekazywane z UE do Japonii będą chronione przez cały cykl ich życia, i zaleciła Komisji dostarczenie dalszych dowodów i wyjaśnień w poruszonych sprawach oraz ścisłe monitorowanie rzeczywistego stosowania przepisów;

V. mając na uwadze, że projektowi decyzji wykonawczej towarzyszy również pismo Ministra Sprawiedliwości z 14 września 2018 r., w którym przywołano dokument sporządzony przez Ministerstwo Sprawiedliwości oraz kilka innych ministerstw i agencji, zatytułowany „Gromadzenie i wykorzystywanie informacji osobowych przez japońskie organy publiczne do celów egzekwowania prawa karnego i bezpieczeństwa narodowego", zawierający przegląd obowiązujących przepisów oraz przedstawione Komisji oficjalne oświadczenia, gwarancje i zobowiązania podpisane na najwyższym szczeblu ministerialnym i agencyjnym, ujęte w załączniku II do decyzji wykonawczej;

1. przyjmuje do wiadomości szczegółową analizę przedstawioną przez Komisję w projekcie decyzji wykonawczej w sprawie odpowiedniego stopnia ochrony, dotyczącą zabezpieczeń, w tym mechanizmów nadzoru i mechanizmów odwoławczych, mających zastosowanie do przetwarzania danych przez podmioty komercyjne, a także dostępu japońskich organów publicznych do danych, zwłaszcza w obszarze egzekwowania prawa i bezpieczeństwa narodowego;

2. zauważa, że Japonia jednocześnie przygotowuje się do uznania poziomu ochrony danych osobowych przekazywanych z Japonii do UE zgodnie z art. 23 ustawy o ochronie informacji osobowych, co oznaczałoby pierwsze w historii dwustronne uznanie równoważności systemów ochrony danych i powstanie największego na świecie obszaru swobodnego i bezpiecznego przepływu danych;

3. z zadowoleniem przyjmuje te zmiany jako przejaw globalnego upowszechniania wysokich standardów ochrony danych; zwraca jednak uwagę, że nie może to w żadnej mierze prowadzić do przyjęcia zasady wzajemności w decyzjach UE stwierdzających odpowiedni stopień ochrony; przypomina, że chcąc przyjąć decyzję stwierdzającą odpowiedni stopień ochrony na mocy RODO, Komisja musi obiektywnie ocenić sytuację prawną i praktyczną w danym państwie trzecim, na danym terytorium, w danym sektorze lub danej organizacji międzynarodowej;

4. zwraca uwagę, że według orzeczenia Trybunału Sprawiedliwości UE „termin »odpowiedni poziom ochrony« nie wymaga identycznego poziomu ochrony, jaki gwarantowany jest w UE, lecz musi być rozumiany jako wymaganie od państwa trzeciego, że zapewnia de facto, na mocy prawa krajowego lub zobowiązań międzynarodowych, poziom ochrony podstawowych praw i wolności zasadniczo równoważny z poziomem ochrony gwarantowanym w Unii Europejskiej na mocy RODO w świetle Karty";

5. zauważa, że prawo do prywatności i do ochrony danych osobowych jest konstytucyjnie gwarantowane zarówno w Japonii, jak i w UE, ale całkowite zbliżenie przepisów UE i Japonii nie będzie możliwe z uwagi na różnice w strukturze konstytucyjnej i w kulturze;

6. odnotowuje wprowadzenie poprawek do ustawy o ochronie informacji osobowych, które weszły w życie 30 maja 2017 r.; z zadowoleniem przyjmuje te istotne ulepszenia;

7. zauważa, że kategorie działalności gospodarczej i przetwarzania, które wyłączono z zakresu ustawy o ochronie informacji osobowych, jednoznacznie wyłączono z zakresu decyzji o stwierdzeniu odpowiedniego poziomu ochrony;

8. uważa, że po przyjęciu w 2016 r. zmienionej ustawy o ochronie informacji osobowych i RODO oba systemy ochrony danych, japoński i unijny, są w wysokim stopniu zbieżne pod względem zasad, zabezpieczeń i praw indywidualnych, a także mechanizmów nadzoru i egzekwowania; zwraca zwłaszcza uwagę na fakt, że na mocy zmienionej ustawy o ochronie informacji osobowych utworzono niezależny organ nadzorczy – Komisję Ochrony Informacji Osobowych;

9. zauważa jednak, że zdaniem samej Komisji Ochrony Informacji Osobowych „pomimo wysokiego stopnia zbieżności między oboma systemami istnieją pewne istotne różnice"; odnotowuje również fakt, że Komisja Ochrony Informacji Osobowych przyjęła 15 czerwca 2018 r. zasady uzupełniające, by zapewnić wyższy poziom ochrony danych osobowych przekazywanych z UE;

10. z zadowoleniem przyjmuje szereg istotnych wyjaśnień zawartych w zasadach uzupełniających, w tym dostosowanie pojęcia „zanonimizowanych informacji osobowych" w ustawie o ochronie informacji osobowych do definicji „informacji anonimowych" zapisanej w RODO;

11. uważa, że dodatkowa ochrona zapisana w zasadach uzupełniających obejmuje tylko przekazywanie danych na mocy decyzji stwierdzających odpowiedni poziom ochrony; przypomina, że ze względu na zakres decyzji stwierdzającej odpowiedni stopień ochrony w niektórych przypadkach przekazywanie danych będzie się odbywać z wykorzystaniem innych dostępnych mechanizmów;

12. przyznaje, że dodatkowa ochrona przewidziana w zasadach uzupełniających dotyczy tylko danych osobowych przekazywanych z Europy, zatem podmioty gospodarcze przetwarzające jednocześnie japońskie i europejskie dane osobowe będą musiały przestrzegać zasad uzupełniających, np. przez zapewnienie środków technicznych („znakowanie elektroniczne") lub organizacyjnych (np. przechowywanie w odrębnej bazie danych), by móc zidentyfikować takie dane osobowe przez cały ich cykl życia; wzywa Komisję, by monitorowała sytuację w celu uniknięcia ewentualnych luk prawnych, które pozwalałyby operatorom obchodzić obowiązki określone w zasadach uzupełniających przez przekazywanie danych za pośrednictwem państw trzecich;

13. zauważa, że z definicji „danych osobowych" w ustawie o ochronie informacji osobowych wyłączono dane „wskazane w zarządzeniu Rady Ministrów jako dane, co do których ze względu na metodę ich wykorzystywania istnieje małe prawdopodobieństwo, że mogą one zaszkodzić prawom i interesom osób fizycznych"; apeluje do Komisji, by oceniła, czy to podejście, bazujące na pojęciu szkody, jest do pogodzenia z podejściem UE, gdzie zakres przepisów o ochronie danych obejmuje wszystkie przypadki przetwarzania danych osobowych; zauważa jednak również, że podejście to byłoby stosowane do bardzo nielicznych sytuacji;

14. zauważa ponadto, że definicja „informacji osobowych" w ustawie o ochronie informacji osobowych odnosi się tylko do informacji umożliwiających „zidentyfikowanie konkretnej osoby"; zwraca również uwagę, że definicja ta nie zawiera wyjaśnień ujętych w RODO, że informacje osobowe należy również traktować jak dane osobowe, jeżeli mogą one posłużyć tylko do „wyodrębnienia" danej osoby, jak wyraźnie stwierdził Trybunał Sprawiedliwości UE;

15. wyraża zaniepokojenie, że węższa definicja „danych osobowych" (oparta na definicji „informacji osobowych") w ustawie o ochronie informacji osobowych może nie wystarczyć do zapewnienia poziomu „merytorycznie równoważnego" z RODO i z orzecznictwem Trybunału Sprawiedliwości UE; w związku z tym kwestionuje zawarte w projekcie decyzji wykonawczej stwierdzenie, że „na mocy ustawy o ochronie informacji osobowych dane UE zawsze będą należeć do kategorii »danych osobowych«"; wzywa Komisję, by w czasie wykonywania decyzji o stwierdzeniu odpowiedniego poziomu ochrony danych osobowych i przy okazji jej okresowego przeglądu ściśle monitorowała praktyczne konsekwencje stosowania różnych pojęć;

16. wzywa Komisję, aby przedstawiła dalsze wyjaśnienia, a w razie potrzeby zwróciła się do władz japońskich o wprowadzenie dalszych wiążących zasad uzupełniających, by zapewnić ochronę wszystkich przekazywanych do Japonii danych osobowych w rozumieniu RODO;

17. z niepokojem zauważa, że w odróżnieniu od prawa UE ani ustawa o ochronie informacji osobowych, ani wytyczne Komisji Ochrony Informacji Osobowych nie zawierają przepisów dotyczących zautomatyzowanego podejmowania decyzji i profilowania, a tylko niektóre przepisy sektorowe odnoszą się do tej kwestii, co nie zapewnia całościowych ogólnych ram prawnych dających materialną, solidną ochronę przed zautomatyzowanym podejmowaniem decyzji i profilowaniem; wzywa Komisję, by wskazała, jak problem ten rozwiązano w japońskich przepisach o ochronie danych, by zapewnić równoważny poziom ochrony; uważa, że sprawa ta nabiera szczególnego znaczenia w świetle niedawnych afer dotyczących profilowania przez Facebook i Cambridge Analytica;

18. uważa, że zgodnie ze wskazówkami EROD stwierdzenie odpowiedniego stopnia ochrony danych zapewnianej przez Japonię wymaga dalszych szczegółowych wyjaśnień w kwestii marketingu bezpośredniego, gdyż ustawa o ochronie informacji osobowych nie zawiera szczegółowych przepisów w tej sprawie;

19. przyjmuje do wiadomości opinię Europejskiej Rady Ochrony Danych, w której wskazano sprawy problematyczne, np. pytanie, czy dane osobowe przekazywane z UE do Japonii będą chronione przez cały cykl ich życia; zwraca się do Komisji o należyte uwzględnienie i przedstawienie w decyzji wykonawczej dalszych dowodów i wyjaśnień wskazujących na istnienie odpowiednich gwarancji;

20. zwraca się do Komisji, by wyjaśniła, czy w przypadku wtórnego przekazywania danych w rozwiązaniu zapisanym w zasadach uzupełniających, wprowadzającym wymóg uzyskania uprzedniej zgody unijnych podmiotów danych na wtórne przekazywanie danych osobom trzecim w obcym kraju, brakuje pewnych istotnych elementów umożliwiającym podmiotom danych wyrażenie zgody, ponieważ nie zdefiniowano jednoznacznie zakresu „informacji o okolicznościach towarzyszących przekazaniu, niezbędnych [podmiotowi danych] do podjęcia decyzji o wyrażeniu zgody", zgodnie z art. 13 RODO, gdyż nie wiadomo np., czy obejmują one informację o państwie trzecim, do którego dane są wtórnie przekazywane; zwraca się do Komisji, by wyjaśniła ponadto ą konsekwencje niewyrażenia przez podmiot danych zgody na wtórne przekazywanie jego danych osobowych;

21. w odniesieniu do skutecznego egzekwowania ustawy o ochronie informacji osobowych wyraża ubolewanie, że poziom grzywien nakładanych przez organy karne jest niewystarczający, by zapewnić faktyczne stosowanie się do ustawy, ponieważ nie wydaje się być proporcjonalny do wagi naruszenia, skuteczny i odstraszający; zauważa jednak, że ustawa o ochronie informacji osobowych przewiduje również sankcje karne, w tym kary pozbawienia wolności; wzywa Komisję do przedstawienia informacji na temat faktycznego stosowania grzywien administracyjnych i sankcji karnych w przeszłości;

22. zauważa, że chociaż Komisja Ochrony Informacji Osobowych nie sprawuje nadzoru nad przetwarzaniem danych w sektorze egzekwowania prawa, to jednak istnieją inne mechanizmy nadzoru, w tym nadzór ze strony niezależnych komisji ds. bezpieczeństwa publicznego w prefekturach; zauważa, że Komisja ds. Nadzoru nad Ujawnianiem Informacji i Ochroną Informacji Osobowych ma pewne uprawnienia w tej dziedzinie, obejmujące przegląd wniosków o dostęp i publikowanie opinii, ale zwraca uwagę, że uprawnienia te nie są prawnie wiążące; z zadowoleniem przyjmuje fakt, że UE i Japonia zgodziły się wprowadzić specjalny mechanizm odwoławczy obsługiwany i nadzorowany przez Komisję Ochrony Informacji Osobowych, który będzie miał zastosowanie do przetwarzania danych osobowych w sektorze egzekwowania prawa i bezpieczeństwa narodowego;

23. zauważa, że zgodnie z japońską ustawą o ochronie informacji osobowych będących w posiadaniu organów administracji podmioty gospodarcze mogą również przekazywać dane organom ścigania na zasadzie „dobrowolności"; zwraca uwagę, że podobnej sytuacji nie przewiduje RODO ani dyrektywa policyjna, i zwraca się do Komisji, by oceniła, czy taki stan faktyczny spełnia wymógwymogu poziomu „merytorycznie równoważnego" z RODO;

24. zna doniesienia medialne na temat japońskiej Dyrekcji ds. SIGINT, „która zatrudnia około 1 700 osób i z co najmniej sześciu obiektów przez całą dobę podsłuchuje rozmowy telefoniczne oraz monitoruje e-maile i inne wiadomości" ([1]); wyraża zaniepokojenie faktem, że o tym elemencie masowej inwigilacji nawet nie wspomniano w projekcie decyzji wykonawczej; wzywa Komisję, by dostarczyła dodatkowe informacje na temat masowej inwigilacji w Japonii; wyraża poważne zaniepokojenie, że ta masowa inwigilacja nie spełnia kryteriów określonych przez Trybunał Sprawiedliwości UE w wyroku w sprawie Schremsa (sprawa C-362/14);

25. wyraża ubolewanie, że dokument „Gromadzenie i wykorzystywanie informacji osobowych przez japońskie organy publiczne do celów egzekwowania prawa karnego i bezpieczeństwa narodowego", zawarty w załączniku II do projektu decyzji wykonawczej, nie ma takiego samego prawnie wiążącego skutku jak zasady uzupełniające;

Podsumowanie

26. wzywa Komisję, by przedstawiła dalsze dowody i wyjaśnienia w wymienionych sprawach, w tym w sprawach wskazanych w opinii Europejskiej Rady Ochrony Danych z 5 grudnia 2018 r., w celu wykazania, że poziom ochrony zapewniany przez japońskie przepisy o ochronie danych jest wystarczający, merytorycznie równoważny z poziomem ochrony, jaką dają europejskie przepisy o ochronie danych;

27. uważa, że decyzja stwierdzająca odpowiedni stopień ochrony może być ponadto wyraźnym sygnałem dla krajów na całym świecie, że spójność z wysokimi unijnymi standardami ochrony danych może dać bardzo wymierne rezultaty; podkreśla w związku z tym znaczenie tej decyzji stwierdzającej odpowiedni stopień ochrony jako precedensu dla przyszłych partnerstw z innymi państwami, które przyjęły nowoczesne przepisy dotyczące ochrony danych;

([1]) Ryan Gallagher, „The Untold Story of Japan's Secret Spy Agency" (Nieznana historia sekretnej japońskiej agencji szpiegowskiej), The Intercept, 19 maja 2018 r., https://theintercept.com/2018/05/19/japan-dfs-surveillance-agency/

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

o

o o

29. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Radzie, Komisji, rządom i parlamentom państw członkowskich, Europejskiej Radzie Ochrony Danych, Europejskiemu Inspektorowi Ochrony Danych, komitetowi powołanemu zgodnie z art. 93 ust. 1 ogólnego rozporządzenia o ochronie danych, Radzie Europy oraz rządowi Japonii.