Piatek, 21 maja 2021 r.

P9_TA(2021)0262

Odpowiednia ochrona danych osobowych przez Zjednoczone Królestwo

Rezolucja Parlamentu Europejskiego z dnia 21 maja 2021 r. w sprawie odpowiedniej ochrony danych osobowych przez Zjednoczone Królestwo (2021/2594(RSP))

(2022/C 15/23)

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 16 lipca 2020 r. w sprawie C-311/18 *Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillian Schrems* (wyrok w sprawie Schrems II) ([1]),

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

— uwzględniając wyrok TSUE z 6 października 2020 r. w sprawie C-623/17 *Privacy International przeciwko Secretary of State of Foreign and Commonwealth affairs* ([3]),

— uwzględniając swoją rezolucję 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 ([4]),

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

— uwzględniając swoją rezolucję z 25 października 2018 r. w sprawie wykorzystania danych użytkowników Facebooka przez Cambridge Analytica oraz wpływu, jaki wywarło to na ochronę danych ([6]),

— uwzględniając swoją rezolucję z dnia 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") ([7]),

— uwzględniając swoją rezolucję z 26 listopada 2020 r. w sprawie przeglądu unijnej polityki handlowej ([8]),

— uwzględniając Umowę o handlu i współpracy z 31 grudnia 2020 r. między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony ([9]),

— uwzględniając swoją rezolucję z 28 kwietnia 2021 r. w sprawie wyniku negocjacji między UE a Zjednoczonym Królestwem ([10]),

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych (ogólne rozporządzenie o ochronie danych) ([11]) (RODO),

---

([1]) ECLI:EU:C:2020:559.
([2]) ECLI:EU:C:2015:650.
([3]) ECLI:EU:C:2020:790.
([4]) Dz.U. C 378 z 9.11.2017, s. 104.
([5]) Dz.U. C 118 z 8.4.2020, s. 133.
([6]) Dz.U. C 345 z 16.10.2020, s. 58.
([7]) Teksty przyjęte, P9_TA(2021)0256.
([8]) Teksty przyjęte, P9_TA(2020)0337.
([9]) Dz.U. L 444 z 31.12.2020, s. 14.
([10]) Teksty przyjęte, P9_TA(2021)0141.
([11]) Dz.U. L 119 z 4.5.2016, s. 1.

— uwzględniając dyrektywę Parlamentu Europejskiego i Rady (UE) 2016/680 z 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 ([12]) (dyrektywa o ochronie danych w sprawach karnych),

— uwzględniając dyrektywę 2002/58/WE Parlamentu Europejskiego i Rady z 12 lipca 2002 r. dotyczącą przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej ([13]),

— uwzględniając wniosek Komisji z 10 stycznia 2017 r. dotyczący rozporządzenia Parlamentu Europejskiego i Rady w sprawie poszanowania życia prywatnego oraz ochrony danych osobowych w łączności elektronicznej (COM(2017)0010)) oraz stanowisko Parlamentu Europejskiego w tej sprawie przyjęte 20 października 2017 r. ([14]),

— uwzględniając zalecenia Europejskiej Rady Ochrony Danych (EROD), w tym jej oświadczenie z 9 marca 2021 r. w sprawie rozporządzenia o prywatności i łączności elektronicznej oraz jej zalecenia nr 1/2020 z 10 listopada 2020 r. w sprawie środków uzupełniających narzędzia przekazywania danych w celu zapewnienia zgodności z unijnym poziomem ochrony danych osobowych,

— uwzględniając dokument „Odpowiedni stopień ochrony przekazywanych danych osobowych" przyjęty 6 lutego 2018 r. przez Grupę Roboczą Art. 29 i zatwierdzony przez EROD,

— uwzględniając zalecenia EROD nr 1/2021 z 2 lutego 2021 r. w sprawie dokumentu „Odpowiedni stopień ochrony przekazywanych danych osobowych" na mocy dyrektywy o ochronie danych w sprawach karnych,

— uwzględniając projekty decyzji stwierdzających odpowiedni stopień ochrony, opublikowane przez Komisję 19 lutego 2021 r. – jedną zgodnie z RODO ([15]), a drugą zgodnie z dyrektywą o ochronie danych w sprawach karnych ([16]),

— uwzględniając opinie EROD nr 14/2021 i 15/2021 z 13 kwietnia 2021 r. w sprawie projektu decyzji wykonawczej Komisji Europejskiej, zgodnie z dyrektywą (UE) 2016/680, w sprawie odpowiedniej ochrony danych osobowych w Zjednoczonym Królestwie,

— uwzględniając europejską konwencję praw człowieka (EKPC) oraz Konwencję Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych, a także protokół zmieniający do niej (tzw. konwencję 108+), których Zjednoczone Królestwo jest stroną,

— uwzględniając rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 182/2011 z 16 lutego 2011 r. ustanawiające przepisy i zasady ogólne dotyczące trybu kontroli przez państwa członkowskie wykonywania uprawnień wykonawczych przez Komisję,

— uwzględniając art. 132 ust. 2 Regulaminu,

— uwzględniając projekt rezolucji Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych,

A. mając na uwadze, że zdolność do transgranicznego przekazywania danych osobowych może być główną siłą napędową innowacji, wydajności i konkurencyjności gospodarczej oraz ma kluczowe znaczenie dla skutecznej współpracy w walce z transgraniczną przestępczością zorganizowaną i poważną przestępczością oraz w walce z terroryzmem, która w coraz większym stopniu zależy od wymiany danych osobowych;

B. mając na uwadze, że w wyroku w sprawie Schrems I TSUE wskazał, że niekontrolowany dostęp organów wywiadowczych do treści wiadomości elektronicznych narusza zasadniczą istotę prawa do poufności komunikacji przewidzianego w art. 7 Karty oraz że Stany Zjednoczone nie zapewniają wystarczających środków prawnych osobom spoza USA przeciwko masowej inwigilacji, co stanowi naruszenie art. 47 Karty;

([12]) Dz.U. L 119 z 4.5.2016, s. 89.
([13]) Dz.U. L 201 z 31.7.2002, s. 37.
([14]) A8-0324/2017.
([15]) Projekt decyzji wykonawczej Komisji na mocy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 w sprawie odpowiedniego stopnia ochrony danych osobowych zapewnianej przez Zjednoczone Królestwo.
([16]) Projekt decyzji wykonawczej Komisji na mocy dyrektywy Parlamentu Europejskiego i Rady (UE) 2016/680 w sprawie odpowiedniego stopnia ochrony danych osobowych zapewnianej przez Zjednoczone Królestwo.

C. mając na uwadze, że Zjednoczone Królestwo od dawna jest ważnym partnerem handlowym wielu państw członkowskich UE, a także bliskim sojusznikiem w dziedzinie bezpieczeństwa; mając na uwadze, że UE i Zjednoczone Królestwo powinny utrzymać tę ścisłą współpracę mimo wystąpienia Zjednoczonego Królestwa z UE, ponieważ będzie to korzystne dla obu stron;

D. mając na uwadze, że europejskie przedsiębiorstwa potrzebują jasności i pewności prawa, ponieważ możliwość transgranicznego przekazywania danych osobowych staje się coraz ważniejsza dla wszystkich rodzajów przedsiębiorstw, które dostarczają towary i świadczą usługi na skalę międzynarodową; mając na uwadze, że decyzja stwierdzająca odpowiedni stopień ochrony w odniesieniu do Zjednoczonego Królestwa na mocy RODO ma ogromne znaczenie, ponieważ wiele europejskich przedsiębiorstw prowadzi handel przez kanał La Manche, zwłaszcza że od brexitu upłynęło niewiele czasu, a przepływy danych w Unii nie podlegają ograniczeniom; mając na uwadze, że nieprzyjęcie solidnych ram dotyczących stopnia ochrony groziłoby zakłóceniem transgranicznego przekazywania danych osobowych w celach handlowych między UE a Zjednoczonym Królestwem oraz wysokimi kosztami przestrzegania przepisów;

E. mając na uwadze, że umowa o handlu i współpracy zawiera szereg zabezpieczeń i warunków wymiany odpowiednich danych w kontekście egzekwowania prawa; mając na uwadze, że negocjacje w sprawie przepływu danych osobowych prowadzono równolegle do negocjacji w sprawie umowy o handlu i współpracy, ale nie zakończono ich do końca okresu przejściowego 31 grudnia 2020 r.; mając na uwadze, że w umowie o handlu i współpracy zawarto klauzulę pomostową jako rozwiązanie przejściowe, którego warunkiem było zobowiązanie się przez Zjednoczone Królestwo, że nie zmieni swojego systemu ochrony danych, aby zapewnić ciągłość przepływów danych osobowych między Zjednoczonym Królestwem a UE do czasu przyjęcia decyzji stwierdzającej odpowiedni stopień ochrony; mając na uwadze, że początkowy czteromiesięczny okres został przedłużony do końca czerwca 2021 r.;

F. mając na uwadze, że ocena przeprowadzona przez Komisję przed przedstawieniem projektu decyzji wykonawczej nie była kompletna ani zgodna z wymogami TSUE dotyczącymi oceny odpowiedniości stopnia ochrony, co EROD podkreśliła w opiniach, w których zaleca Komisji dalszą ocenę konkretnych aspektów prawa lub praktyki Zjednoczonego Królestwa dotyczących hurtowego gromadzenia danych, ujawniania danych za granicę i umów międzynarodowych w dziedzinie wymiany danych wywiadowczych, dodatkowego wykorzystywania informacji gromadzonych do celów egzekwowania prawa oraz niezależności komisarzy sądowych;

G. mając na uwadze, że Komisja nie uwzględniła niektórych aspektów prawa lub praktyki Zjednoczonego Królestwa, czego skutkiem jest niespójność projektów decyzji wykonawczych z prawem UE; mając na uwadze, że zgodnie z art. 45 RODO Komisja, oceniając, czy poziom ochrony jest odpowiedni, uwzględnia w szczególności „(…) 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, a także wdrażanie takiego ustawodawstwa, zasady ochrony danych osobowych, zasady dotyczące wykonywania zawodu, środki bezpieczeństwa, w tym zasady dalszego przekazywania danych osobowych do kolejnego państwa trzeciego lub innej organizacji międzynarodowej, których przestrzega się w tym państwie lub w organizacji międzynarodowej, orzecznictwo" oraz „(…) międzynarodowe zobowiązania zaciągnięte przez dane państwo trzecie lub daną organizację międzynarodową lub inne obowiązki wynikające z prawnie wiążących konwencji lub instrumentów oraz z udziału w systemach wielostronnych lub regionalnych, w szczególności w dziedzinie ochrony danych osobowych", co obejmuje umowy międzynarodowe w innych dziedzinach wiążące się z dostępem do danych lub wymianą informacji, a zatem wymaga oceny takich umów;

H. mając na uwadze, że w wyroku w sprawie Schrems I TSUE wyraźnie stwierdził, że „przy badaniu poziomu ochrony zapewnionego w państwie trzecim Komisja zobowiązana jest ocenić treść reguł mających zastosowanie w tym państwie wynikających z jego ustawodawstwa wewnętrznego lub ze zobowiązań międzynarodowych, a także praktykę zmierzającą do zapewnienia poszanowania tych reguł, przy czym instytucja ta powinna zgodnie z art. 25 ust. 2 dyrektywy 95/46/WE wziąć pod uwagę wszystkie okoliczności dotyczące przekazywania danych osobowych do państwa trzeciego" (pkt 75);

I. mając na uwadze, że działania służb wywiadowczych i wymiana informacji z państwami trzecimi są zgodnie z traktatami wyłączone z zakresu stosowania prawa UE w odniesieniu do państw członkowskich i że objęto je niezbędną oceną odpowiedniości poziomu ochrony danych osobowych zapewnianego przez państwa trzecie, co potwierdził TSUE w wyrokach w sprawach Schrems I i II;

J. mając na uwadze, że standardy ochrony danych opierają się nie tylko na obowiązujących przepisach, lecz także na ich stosowaniu w praktyce, oraz mając na uwadze, że przygotowując decyzję, Komisja oceniła jedynie przepisy, a nie ich stosowanie w praktyce;

K. mając na uwadze, że Komisja uznaje, że odpowiednią ochronę na mocy RODO zapewnia obecnie 12 państw trzecich, a niedawno zakończyła rozmowy z Republiką Korei; mając na uwadze, że Zjednoczone Królestwo to pierwszy kraj, w odniesieniu do którego Komisja zaproponowała uznanie stopnia ochrony za odpowiedni na mocy dyrektywy o ochronie danych w sprawach karnych;

L. mając ma uwadze, że przypadek Zjednoczonego Królestwa różni się od wszystkich wcześniejszych ocen odpowiedniości stopnia ochrony, ponieważ dotyczy byłego państwa członkowskiego UE, które w pełni włączyło przepisy RODO do swojego prawa krajowego, a ponadto przewidziało, że całe „ustawodawstwo krajowe wywodzące się z przepisów UE", w tym przepisy transponujące dyrektywę o ochronie danych w sprawach karnych, będzie nadal miało zastosowanie po zakończeniu okresu przejściowego;

I. **OGÓLNE ROZPORZĄDZENIE O OCHRONIE DANYCH**

Uwagi ogólne

1. zwraca uwagę, że Zjednoczone Królestwo jest sygnatariuszem EKPC oraz Konwencji Rady Europy o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych; oczekuje, że Zjednoczone Królestwo zapewni takie same minimalne ramy ochrony danych pomimo wystąpienia z Unii Europejskiej;

2. z zadowoleniem przyjmuje zobowiązanie Zjednoczonego Królestwa do poszanowania demokracji i praworządności oraz do ochrony praw podstawowych, takich jak te określone w EKPC, w tym wysokiego poziomu ochrony danych, i nadania im mocy wiążącej na szczeblu krajowym; przypomina, że jest to niezbędny warunek wstępny współpracy UE ze Zjednoczonym Królestwem; przypomina, że chociaż art. 8 EKPC dotyczący prawa do prywatności stanowi część prawa krajowego Zjednoczonego Królestwa na mocy ustawy o prawach człowieka z 1998 r. i prawa zwyczajowego w związku z wprowadzeniem nowej kategorii czynu niedozwolonego polegającego na niewłaściwym wykorzystywaniu informacji dotyczących życia prywatnego, wysiłki na rzecz uwzględnienia podstawowego prawa do ochrony danych zostały odrzucone przez rząd w głosowaniu;

3. zwraca uwagę, że przy opracowywaniu solidnych zasad ochrony danych w RODO UE wybrała podejście do zarządzania danymi koncentrujące się na prawach człowieka, dlatego wyraża głębokie zaniepokojenie publicznymi oświadczeniami premiera Zjednoczonego Królestwa, który oznajmił, że Zjednoczone Królestwo będzie dążyć do odejścia od unijnych przepisów o ochronie danych i do ustanowienia własnych „suwerennych" kontroli w tej dziedzinie; uważa, że krajowa strategia Zjednoczonego Królestwa na 2020 r. dotycząca danych odbiega od zasady ochrony danych osobowych na rzecz szerszego wykorzystywania i udostępniania danych, co jest niezgodne z zasadami sprawiedliwości, minimalizacji danych i celowości określonymi w RODO; zauważa, że w swoich opiniach dotyczących odpowiedniości stopnia ochrony EROD podkreśliła, że może to zagrażać ochronie danych osobowych przekazywanych z UE;

4. zwraca uwagę, że ważne decyzje stwierdzające odpowiedni stopień ochrony znacznie zwiększają ochronę praw podstawowych osób fizycznych i pewność prawa dla przedsiębiorstw; podkreśla jednak, że decyzje stwierdzające odpowiedni stopień ochrony oparte na niepełnych ocenach i nieegzekwowane odpowiednio przez Komisję mogą przynieść odwrotny skutek, jeżeli zostaną podważone w sądzie;

5. wskazuje, że ocena przeprowadzona przez Komisję przed przedstawieniem projektu decyzji wykonawczej nie była kompletna ani zgodna z wymogami TSUE dotyczącymi oceny odpowiedniości stopnia ochrony, co EROD podkreśliła w opiniach, w których zaleca Komisji dalszą ocenę konkretnych aspektów prawa lub praktyki Zjednoczonego Królestwa dotyczących hurtowego gromadzenia danych, ujawniania danych za granicę i umów międzynarodowych w dziedzinie wymiany danych wywiadowczych, dodatkowego wykorzystywania informacji gromadzonych do celów egzekwowania prawa oraz niezależności komisarzy sądowych;

Wykonanie RODO

6. wyraża zaniepokojenie z powodu niedostatecznego wykonania, a często braku wykonania RODO przez Zjednoczone Królestwo, gdy było ono jeszcze członkiem UE; wskazuje w szczególności, że w przeszłości Biuro Komisarza ds. Informacji w Zjednoczonym Królestwie nie stosowało odpowiednio przepisów; zwraca uwagę na przykład komisarza ds. informacji, który zamknął skargę dotyczącą technologii reklamowej po zorganizowaniu dwóch wydarzeń z udziałem zainteresowanych podmiotów i sporządził raport aktualizujący („Update Report on Adtech"), w którym stwierdził, że „rozumienie wymogów ochrony danych przez branże technologii reklamowej wydaje się niedojrzałe", ale nie skorzystał ze swoich

uprawnień w zakresie egzekwowania prawa ([17]); jest zaniepokojony, że nieegzekwowanie przepisów jest problemem strukturalnym, co przyznano w polityce regulacyjnej komisarza ds. informacji, w której wyraźnie stwierdzono, że „w większości przypadków komisarz będzie korzystać ze swoich uprawnień tylko w najpoważniejszych przypadkach, stanowiących najcięższe naruszenie obowiązków w zakresie praw do informacji. Są to zazwyczaj działania umyślne lub wynikające z zaniedbania, lub powtarzające się naruszenia obowiązków w zakresie praw do informacji, powodujące szkody dla osób fizycznych"; podkreśla, że w praktyce oznacza to, że nie usunięto wielu naruszeń prawa o ochronie danych w Zjednoczonym Królestwie;

7. odnotowuje krajową strategię Zjednoczonego Królestwa dotyczącą danych, zaktualizowaną 9 grudnia 2020 r., która zapowiada odejście od ochrony danych osobowych na rzecz szerszego wykorzystywania i udostępniania danych; zwraca uwagę, że zawarte w strategii stanowisko, iż „nieprzekazywanie danych może negatywnie wpłynąć na społeczeństwo", jest niezgodne z zasadami minimalizacji danych i celowości określonymi w RODO i prawie pierwotnym;

8. zauważa, że Komisja Spraw Konstytucyjnych w 2004 r. ([18]) oraz Komisja Spraw Publicznych parlamentu Zjednoczonego Królestwa w 2014 r. ([19]) zaleciły zapewnienie niezależności komisarza ds. informacji dzięki temu, że miałby on być urzędnikiem parlamentu, odpowiedzialnym przed parlamentem, a nie powoływanym nadal przez ministra ds. mediów cyfrowych i sportu; ubolewa, że nie zastosowano się do tego zalecenia;

Przetwarzanie danych do celów kontroli imigracyjnej

9. odnotowuje, że prawo Zjednoczonego Królestwa o ochronie danych zawiera odstępstwo od niektórych aspektów podstawowych praw i zasad ochrony danych, takich jak prawo dostępu i prawo osoby, której dane dotyczą, do uzyskania informacji, komu udostępniono jej dane, jeżeli taka ochrona „byłaby ze szkodą dla skutecznej kontroli imigracyjnej"; podkreśla, że monitorowanie i prawidłowe stosowanie tego odstępstwa musi być zgodne ze standardami adekwatności, obejmującymi wymóg uwzględnienia praktyki i zasady, oraz zaznacza, że „konieczne jest rozważenie nie tylko treści przepisów mających zastosowanie do danych osobowych przekazywanych do państwa trzeciego (…), ale również istniejącego systemu zapewniającego skuteczność takich przepisów"; uznaje, że odstępstwo to, z którego mogą korzystać wszyscy administratorzy danych w Zjednoczonym Królestwie, zostało zatwierdzone przez Biuro Komisarza ds. Informacji i sąd, oraz że można powoływać się na nie wyłącznie w indywidualnych przypadkach i stosować je w razie konieczności i w sposób proporcjonalny; przypomina o ujawnionych niedawno informacjach, według których złożono 17 780 wniosków o udzielenie dostępu do danych przetworzonych przez Ministerstwo Spraw Wewnętrznych od 1 kwietnia 2018 r. do 31 marca 2019 r., dotyczących 146,75 mln osób, a odstępstwo imigracyjne zostało zastosowane w ponad 70 % wniosków osób, których dane dotyczą, skierowanych do Ministerstwa Spraw Wewnętrznych w 2020 r. ([20]); podkreśla, że nawet w przypadkach, w których Ministerstwo Spraw Wewnętrznych skorzystało z tego odstępstwa, dostępu do informacji nie odmówiono całkowicie, a ograniczono go do zredagowanych dokumentów;

10. zwraca uwagę, że odstępstwo to ma obecnie zastosowanie do obywateli UE, którzy mieszkają lub planują zamieszkać w Zjednoczonym Królestwie; jest głęboko zaniepokojony faktem, że odstępstwo pozbawia osoby, których dotyczy, głównych możliwości w zakresie rozliczalności i środków zaradczych, i podkreśla, że nie jest to odpowiedni poziom ochrony;

([17]) Lomas, N., *UK's ICO faces legal action after closing adtech complaint with nothing to show for it*, TechCrunch, San Francisco, 2020.

([18]) Siódme sprawozdanie Komisji Specjalnej ds. Konstytucyjnych, opublikowane przez Izbę Gmin 13 czerwca 2006 r. Ust. 108 stanowi: „Dostrzegamy ogromne korzyści tego, by komisarz ds. informacji był odpowiedzialny bezpośrednio przed parlamentem i finansowany przez parlament, oraz zalecamy rozważenie takiej zmiany przy okazji nowelizacji odnośnych przepisów".

([19]) Sprawozdanie Komisji Administracji Publicznej pt. „Kto ponosi odpowiedzialność? Relacje między rządem a organami publicznymi", opublikowane przez Izbę Gmin 4 listopada 2014 r. Ust. 64 stanowi: „Komisarz ds. informacji i Inspektorat Służby Więziennej powinni być w pełni niezależni od rządu i powinni odpowiadać przed parlamentem. Komisarz ds. informacji, komisarz ds. nominacji publicznych oraz przewodniczący Komisji ds. Standardów w Życiu Publicznym powinni zostać urzędnikami parlamentu, podobnie jak ma to już miejsce w przypadku rzecznika praw obywatelskich ds. parlamentarnych i służby zdrowia oraz kontrolera i audytora generalnego".

([20]) Komunikat prasowy grupy Open Rights z 3 marca 2021 r. pt. „Documents reveal controversial Immigration Exemption used in 70 % of access requests to Home Office" [„Dokumenty ujawniają kontrowersyjne odstępstwo imigracyjne stosowane w 70 % wniosków o dostęp do danych skierowanych do Ministerstwa Spraw Wewnętrznych"].

11. ponownie wyraża poważne zaniepokojenie stosowanym w polityce imigracyjnej Zjednoczonego Królestwa odstępstwem odnoszącym się do praw osób, których dane dotyczą; przypomina swoje stanowisko, zgodnie z którym odstępstwo dotyczące przetwarzania danych osobowych do celów imigracyjnych przewidziane w brytyjskiej ustawie o ochronie danych musi zostać zmienione przed wydaniem ważnej decyzji stwierdzającej odpowiedni stopień ochrony, co Parlament już wielokrotnie wyrażał np. w rezolucji z 12 lutego 2020 r. w sprawie propozycji mandatu dotyczącego negocjacji w sprawie nowego partnerstwa ze Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej ([21]) oraz w opinii Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych z 5 lutego 2021 r. ([22]); wzywa Komisję, aby dążyła do zniesienia odstępstwa imigracyjnego lub zapewniła jego reformę, tak by to odstępstwo i jego stosowanie dawało wystarczające zabezpieczenia osobom, których dane dotyczą, i nie naruszało standardów oczekiwanych od państw trzecich;

Masowa inwigilacja

12. przypomina o ujawnionych przez sygnalistę Edwarda Snowdena informacjach dotyczących masowej inwigilacji prowadzonej przez Stany Zjednoczone i Zjednoczone Królestwo; przypomina, że brytyjski program „Tempora" prowadzony przez Urząd ds. Komunikacji w rządzie Zjednoczonego Królestwa (GCHQ) przechwytuje komunikację w czasie rzeczywistym za pośrednictwem szkieletowych kabli światłowodowych i rejestruje dane, aby można je było później przetwarzać i przeszukiwać; przypomina, że ta masowa inwigilacja treści komunikacyjnych i metadanych nie opiera się na konkretnych podejrzeniach ani na targetowaniu;

13. przypomina, że w wyrokach w sprawie Schrems I i Schrems II TSUE orzekł, że masowy dostęp do treści prywatnych komunikatów dotyczy istoty prawa do prywatności oraz że w takich przypadkach test konieczności i proporcjonalności nie jest już wymagany; podkreśla, że zasady te mają zastosowanie do przekazywania danych do państw trzecich innych niż USA, w tym do Zjednoczonego Królestwa;

14. przypomina swoją rezolucję z 12 marca 2014 r., zgodnie z którą programy masowej inwigilacji prowadzone przez brytyjską agencję wywiadu GCHQ w sposób nieograniczony i nieoparty na podejrzeniach są niezgodne z zasadami konieczności i proporcjonalności w społeczeństwie demokratycznym i z prawem UE o ochronie danych; uznaje, że od tego czasu Zjednoczone Królestwo znacząco zreformowało przepisy dotyczące nadzoru oraz wprowadziło zabezpieczenia, które wykraczają poza warunki określone przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE) w wyroku w sprawie Schrems II ([23]), i zabezpieczenia przewidziane w przepisach dotyczących nadzoru większości państw członkowskich; z zadowoleniem przyjmuje w szczególności zapewnienie pełnego dostępu do skutecznych sądowych środków odwoławczych; przypomina, że specjalny sprawozdawca ONZ ds. prawa do prywatności z zadowoleniem przyjął solidne zabezpieczenia wprowadzone ustawą o uprawnieniach dochodzeniowych z 2016 r. pod względem konieczności, proporcjonalności i niezależnego zezwolenia organu sądowego;

15. przypomina, że we wrześniu 2018 r. Europejski Trybunał Praw Człowieka potwierdził, iż brytyjskie programy masowego przechwytywania i zatrzymywania danych, w tym Tempora, są „nielegalne i niezgodne z warunkami niezbędnymi dla istnienia demokratycznego społeczeństwa" ([24]);

16. uważa za niedopuszczalne, że projekt decyzji stwierdzających odpowiedni stopień ochrony nie uwzględnia ani braku ograniczeń uprawnień Zjednoczonego Królestwa w zakresie danych masowych, ani faktycznego wykorzystywania operacji inwigilacji prowadzonych przez Zjednoczone Królestwo i Stany Zjednoczone, ujawnionych przez Edwarda Snowdena, w tym następujących faktów:

a) brak jest skutecznego nadzoru merytorycznego ze strony komisarza ds. informacji lub sądów nad stosowaniem wyłączenia dotyczącego bezpieczeństwa narodowego w brytyjskim prawie o ochronie danych;

b) ograniczenia w korzystaniu z „masowych uprawnień" w Zjednoczonym Królestwie nie są określone w samej ustawie, czego wymaga TSUE (ale raczej pozostawia się je w gestii władzy wykonawczej podlegającej „stosownej" kontroli sądowej);

([21]) Teksty przyjęte, P9_TA(2020)0033.

([22]) Opinia Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w sprawie zawarcia, w imieniu Unii, Umowy o handlu i współpracy między Unią Europejską i Europejską Wspólnotą Energii Atomowej, z jednej strony, a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej, z drugiej strony, oraz Umowy między Unią Europejską a Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej w sprawie procedur bezpieczeństwa na potrzeby wymiany i ochrony informacji niejawnych, LIBE_AL(2021)680848.

([23]) Wyrok z 16 lipca 2020 r., Data Protection Commissioner przeciwko Facebook Ireland Limited i Maximillianowi Schremsowi, C-311/18, ECLI:EU:C:2020:559.

([24]) Wyrok Europejskiego Trybunału Praw Człowieka z 13 września 2018 r. w sprawie Big Brother Watch i in. przeciwko Zjednoczonemu Królestwu, skargi nr 58170/13, 62322/14, 24960/15.

c) opis „danych wtórnych" (metadanych) w projektach decyzji jest w bardzo mylący i nie uwzględnia faktu, że mogą one ujawniać wiele informacji i być niezmiernie inwazyjne oraz podlegają wyrafinowanym zautomatyzowanym analizom (jak TSUE stwierdził w wyroku w sprawie *Digital Rights Ireland* ([25])), jednak zgodnie z prawem Zjednoczonego Królestwa metadane nie są w znaczący sposób chronione przed niewłaściwym dostępem, hurtowym gromadzeniem i analizą opartą na sztucznej inteligencji przez brytyjskie agencje wywiadowcze;

d) agencje należące do sojuszu „pięciorga oczu", w szczególności GCHQ i Agencja Bezpieczeństwa Narodowego (NSA), w praktyce dzielą się wszystkimi danymi wywiadowczymi;

zwraca ponadto uwagę, że w przypadku Stanów Zjednoczonych obywatele Zjednoczonego Królestwa podlegają pewnym nieformalnym gwarancjom uzgodnionym między GCHQ a NSA; wyraża głębokie zaniepokojenie faktem, że zabezpieczenia te nie chroniłyby obywateli ani mieszkańców UE, których dane mogą być dalej przekazywane lub udostępniane NSA;

17. wzywa państwa członkowskie do zawierania ze Zjednoczonym Królestwem umów o zakazie szpiegowania i apeluje do Komisji, aby wykorzystała wymianę informacji ze swoimi odpowiednikami ze Zjednoczonego Królestwa do przekazania, że jeżeli brytyjskie przepisy i praktyki w zakresie nadzoru nie zostaną zmienione, jedyną wykonalną możliwością ułatwienia podejmowania decyzji stwierdzających odpowiedni stopień ochrony byłoby zawarcie z państwami członkowskimi umów o zakazie szpiegowania;

Dalsze przekazywanie informacji

18. podkreśla, że ustawa z 2018 r. o wystąpieniu z Unii Europejskiej stanowi, iż orzecznictwo TSUE wydane przed zakończeniem okresu przejściowego stanie się „utrzymanymi przepisami prawa UE", więc tym samym będzie prawnie wiążące dla Zjednoczonego Królestwa; zwraca uwagę, że przy ocenie adekwatności innych państw trzecich Zjednoczone Królestwo jest związane zasadami i warunkami określonymi w wyrokach TSUE w sprawach Schrems I i Schrems II; jest jednak zaniepokojony, że sądy Zjednoczonego Królestwa nie będą już stosowały Karty; zwraca uwagę, że Zjednoczone Królestwo nie podlega już jurysdykcji TSUE, który jest najwyższą instancją dokonującą wykładni Karty;

19. zwraca uwagę, że zgodnie z wykładnią TSUE brytyjskie przepisy dotyczące udostępniania danych osobowych na mocy ustawy o gospodarce cyfrowej z 2017 r. i dalszego przekazywania danych naukowych w widoczny sposób nie są „zasadniczo równoważne" z przepisami określonymi w RODO;

20. jest zaniepokojony tym, że Zjednoczone Królestwo przyznało sobie prawo do oświadczenia, że inne państwa lub terytoria trzecie zapewniają odpowiednią ochronę danych niezależnie od tego, czy UE uważa dane państwo lub terytorium trzecie za zapewniające taką ochronę; przypomina, że Zjednoczone Królestwo oświadczyło już, iż Gibraltar zapewnia taką ochronę, mimo że UE tego nie uczyniła; jest głęboko zaniepokojony, że status Zjednoczonego Królestwa w zakresie odpowiedniego stopnia ochrony prowadziłby w związku z tym do obchodzenia przepisów UE dotyczących przekazywania danych do państw lub terytoriów nie uznawanych za odpowiednie na mocy prawa UE;

21. odnotowuje, że 1 lutego 2021 r. Zjednoczone Królestwo przesłało wniosek w sprawie przystąpienia do Kompleksowego i Progresywnego Partnerstwa Transpacyficznego (CPTTP), w szczególności w celu „czerpania korzyści z nowoczesnych zasad handlu elektronicznego, które umożliwiają swobodny przepływ danych między członkami, usunięcie niepotrzebnych barier dla przedsiębiorstw [itd.]"; z niepokojem zauważa, że w przypadku ośmiu z jedenastu członków partnerstwa CPTTP Unia Europejska nie wydała decyzji stwierdzającej odpowiedni stopień ochrony; jest głęboko zaniepokojony ewentualnym dalszym przekazywaniem do tych państw danych osobowych obywateli i mieszkańców UE, jeżeli Zjednoczonemu Królestwu zostanie wydana decyzja stwierdzająca odpowiedni stopień ochrony ([26]);

([25]) Wyrok Trybunału Sprawiedliwości z 8 kwietnia 2014 r. w sprawach C-293/12 i C-594/12 Digital Rights Ireland Ltd przeciwko Minister for Communications, Marine and Natural Resources i in. oraz Kärntner Landesregierung i in., ECLI:EU:C:2014:238.

([26]) Komunikat prasowy brytyjskiego Departamentu Handlu Międzynarodowego z 30 stycznia 2021 r. pt. „Zjednoczone Królestwo ubiega się o członkostwo w ogromnej strefie wolnego handlu CPTPP".

22. ubolewa, że Komisja nie oceniła wpływu i potencjalnych zagrożeń związanych z kompleksową umową o partnerstwie gospodarczym między Zjednoczonym Królestwem Wielkiej Brytanii i Irlandii Północnej a Japonią, która zawiera postanowienia dotyczące danych osobowych i poziomu ochrony danych;

23. wyraża zaniepokojenie faktem, że gdyby Zjednoczone Królestwo włączało przepisy dotyczące przekazywania danych do przyszłych umów handlowych, między innymi umów handlowych między Stanami Zjednoczonymi a Zjednoczonym Królestwem, naruszałoby to poziom ochrony zapewniany przez RODO;

II. ***DYREKTYWA O OCHRONIE DANYCH W SPRAWACH KARNYCH***

24. podkreśla, że Zjednoczone Królestwo jest pierwszym państwem, w przypadku którego Komisja zasugerowała przyjęcie na mocy dyrektywy (UE) 2016/680 decyzji stwierdzającej odpowiedni stopień ochrony;

25. odnotowuje umowę Zjednoczonego Królestwa ze Stanami Zjednoczonymi o transgranicznym dostępie do danych ([27]), podpisaną na mocy amerykańskiej ustawy CLOUD, która ułatwia przekazywanie danych do celów egzekwowania prawa; jest głęboko zaniepokojony faktem, że umożliwi to władzom USA nieuprawniony dostęp do danych osobowych obywateli i mieszkańców UE; podziela obawy EROD, że zabezpieczenia przewidziane w umowie parasolowej między UE a USA ([28]), stosowane mutatis mutandis, mogą nie spełniać kryteriów jasności, precyzji i dostępności przepisów, jeśli chodzi o dostęp do danych osobowych, lub mogą być niewystarczająco umocowane, by były skuteczne i egzekwowalne na podstawie prawa brytyjskiego;

26. przypomina, że wyrok TSUE w sprawie C-623/17 należy interpretować w ten sposób, iż uniemożliwia on przyjmowanie przepisów krajowych, które zezwalałyby organom państwowym na wymaganie od dostawców usług łączności elektronicznej ogólnego i niezróżnicowanego przesyłania danych o ruchu i danych o lokalizacji do państwowych agencji bezpieczeństwa i wywiadu do celów ochrony bezpieczeństwa narodowego;

27. zauważa, że w tym przypadku TSUE uznał za nielegalne gromadzenie danych masowych w Zjednoczonym Królestwie na mocy ustawy z 2000 r. regulującej uprawnienia śledcze; zwraca uwagę, że w międzyczasie ustawę tę zastąpiono ustawą o uprawnieniach śledczych (ustawa IPA z 2016 r.) w celu wzmocnienia zasad konieczności i proporcjonalności; podkreśla, że w ramach ustawy IPA z 2016 r. przechwytywanie podlega nadzorowi sądowemu i umożliwia osobom fizycznym dostęp do dotyczących ich danych oraz składanie skarg do sądu ds. uprawnień dochodzeniowych; ubolewa jednak nad faktem, że ustawa IPA z 2016 r. nadal umożliwia praktykę gromadzenia danych masowych;

28. jest zaniepokojony niedawnymi doniesieniami, według których system gromadzenia i zatrzymywania danych masowych jest częścią działań próbnych prowadzonych przez brytyjskie Ministerstwo Spraw Wewnętrznych w ramach ustawy IPA z 2016 r.;

29. przypomina, że w swojej rezolucji z dnia 12 lutego 2020 r. Parlament Europejski podkreślił, że „Zjednoczone Królestwo nie może mieć bezpośredniego dostępu do danych z unijnych systemów informacyjnych ani uczestniczyć w strukturach zarządzania agencjami UE w obszarze wolności, bezpieczeństwa i sprawiedliwości, a przekazywanie Zjednoczonemu Królestwu informacji, w tym danych osobowych, powinno podlegać rygorystycznym zabezpieczeniom, kontroli i nadzorowi obejmującym poziom ochrony danych osobowych równoważny poziomowi zapewnianemu przez prawo UE"; odnotowuje niedociągnięcia stwierdzone w sposobie, w jaki Zjednoczone Królestwo wdrożyło przepisy o ochronie danych, gdy było jeszcze państwem członkowskim UE; przypomina, że Zjednoczone Królestwo rejestrowało i prowadziło kopię Systemu Informacyjnego Schengen (SIS); oczekuje, że organy ścigania Zjednoczonego Królestwa będą w pełni przestrzegać obowiązujących przepisów przy wymianie danych osobowych w przyszłości; przypomina, że Zjednoczone Królestwo zachowuje dostęp do niektórych unijnych baz danych dotyczących egzekwowania prawa – wyłącznie do wyników typu trafienie/brak trafienia – i jest prawnie wykluczone z dostępu do SIS;

([27]) Umowa między rządem Zjednoczonego Królestwa Wielkiej Brytanii i Irlandii Północnej a rządem Stanów Zjednoczonych Ameryki z 3 października 2019 r. w sprawie dostępu do danych elektronicznych do celów zwalczania poważnej przestępczości.

([28]) Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską w sprawie ochrony informacji osobowych powiązanych z zapobieganiem przestępczości, prowadzeniem postępowań przygotowawczych, wykrywaniem i ściganiem czynów zabronionych, Dz.U. L 336 z 10.12.2016, s. 3.

30. wyraża zaniepokojenie doniesieniami ze stycznia 2021 r., według których 400 000 rejestrów karnych zostało przypadkowo usuniętych z brytyjskiego Krajowego Komputera Policyjnego; zaznacza, że nie wzbudza to zaufania do wysiłków Zjednoczonego Królestwa w zakresie ochrony danych na potrzeby egzekwowania prawa;

31. zauważa, że w projekcie decyzji stwierdzającej odpowiedni stopień ochrony dogłębnie oceniono prawa każdego organu Zjednoczonego Królestwa, który jest upoważniony prawem krajowym do przechwytywania i zatrzymywania danych osobowych ze względów bezpieczeństwa narodowego; ponadto z zadowoleniem odnotowuje, że szczegółowe sprawozdania z nadzoru dotyczące organów odpowiedzialnych za wspólnotę wywiadowczą zawierają informacje o aktualnych praktykach inwigilacyjnych Zjednoczonego Królestwa; wzywa Komisję, aby nadal oceniała i monitorowała rodzaje danych komunikacyjnych, które wchodzą w zakres brytyjskich uprawnień do zatrzymywania danych i ich legalnego przechwytywania;

32. zwraca uwagę, że umowa o handlu i współpracy między Unią Europejską a Zjednoczonym Królestwem obejmuje tytuły dotyczące wymiany danych DNA, odcisków palców i danych rejestracyjnych pojazdów, przekazywanie i przetwarzanie danych dotyczących przelotu pasażera (PNR), współpracę w zakresie informacji operacyjnych oraz współpracę z Europolem i Eurojustem, które będą miały zastosowanie niezależnie od decyzji stwierdzającej odpowiedni stopień ochrony; przypomina jednak o obawach – wyrażonych w opinii Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych z lutego 2021 r. w sprawie umowy o handlu i współpracy – co do prawa do specjalnego wykorzystywania i dłuższego zatrzymywania danych osobowych, przyznanego Zjednoczonemu Królestwu na mocy ram prawnych z Prüm i tytułów umowy o handlu i współpracy dotyczących danych PNR, które to prawo nie jest zgodne z zasadami wykorzystywania i zatrzymywania danych przez państwa członkowskie; przypomina o prawie do wystąpienia do TSUE o weryfikację zgodności proponowanej umowy międzynarodowej z prawem, a w szczególności jej zgodności z ochroną praw podstawowych ([29]);

Podsumowanie

33. wzywa Komisję, aby zagwarantowała unijnym przedsiębiorstwom, że decyzja stwierdzająca odpowiedni stopień ochrony zapewni solidną, wystarczającą i zorientowaną na przyszłość podstawę prawną przekazywania danych; podkreśla, że należy dopilnować, aby tę decyzję stwierdzającą odpowiedni stopień ochrony uznano za możliwą do zaakceptowania, jeżeli TSUE miałby przeprowadzić jej przegląd, i zaznacza, że należy zatem uwzględnić wszystkie zalecenia zawarte w opinii EROD;

34. z zadowoleniem odnotowuje, że decyzje stwierdzające odpowiedni stopień ochrony będą obowiązywać tylko przez cztery lata, gdyż Zjednoczone Królestwo – teraz, kiedy nie jest już państwem członkowskim UE – może zdecydować się na zmianę przepisów z zastrzeżeniem przeprowadzenia przez Komisję oceny odpowiedniości stopnia ochrony; wzywa Komisję, aby w międzyczasie nadal monitorowała poziom ochrony danych w Zjednoczonym Królestwie pod względem prawnym i praktycznym oraz przeprowadziła dogłębną ocenę, zanim odnowi decyzję stwierdzającą odpowiedni stopień ochrony w 2025 r.;

35. jest zdania, że przyjmując obie decyzje wykonawcze, które są niezgodne z prawem UE, bez rozwiązania wszystkich kwestii wymienionych w niniejszej rezolucji, Komisja wykracza poza uprawnienia wykonawcze przyznane jej na mocy rozporządzenia (UE) 2016/679 i dyrektywy (UE) 2016/680; w związku z tym sprzeciwia się przyjęciu obu aktów wykonawczych, ponieważ projekty decyzji wykonawczych są niezgodne z prawem UE;

36. wzywa Komisję do zmiany obu projektów decyzji wykonawczych w celu zapewnienia ich pełnej zgodności z prawem i orzecznictwem UE;

37. zwraca się do krajowych organów ochrony danych, aby zawiesiły przekazywanie danych osobowych, które mogłyby podlegać nieograniczonemu dostępowi brytyjskich organów wywiadowczych, gdyby Komisja przyjęła decyzje stwierdzające odpowiedni stopień ochrony w odniesieniu do Zjednoczonego Królestwa, zanim rozwiąże ono wyżej wspomniane kwestie;

38. wzywa Komisję i właściwe organy Zjednoczonego Królestwa, aby opracowały plan działania w celu jak najszybszego zaradzenia brakom stwierdzonym w opiniach EROD i innym nierozwiązanym problemom w zakresie ochrony danych w Zjednoczonym Królestwie, co musi być warunkiem wstępnym przyjęcia ostatecznej decyzji stwierdzającej odpowiedni stopień ochrony;

39. wzywa Komisję, aby nadal ściśle monitorowała poziom ochrony danych, a także przepisy i praktyki dotyczące masowej inwigilacji w Zjednoczonym Królestwie; wskazuje, że rozdział V RODO przewiduje inne prawne możliwości przekazywania danych osobowych Zjednoczonemu Królestwu; przypomina, że zgodnie z wytycznymi EROD przekazywanie danych w oparciu o odstępstwa w szczególnych sytuacjach na podstawie art. 49 RODO musi mieć charakter wyjątkowy;

([29]) Rezolucja Parlamentu Europejskiego w sprawie projektu decyzji Komisji określającej odpowiedni poziom ochrony danych osobowych dotyczących przelotu pasażera (PNR) przekazywanych do Amerykańskiego Biura Ceł i Ochrony Granic (Dz.U. C 103 E z 29.4.2004, s. 665).

40. ubolewa, że Komisja zignorowała apele Parlamentu o zawieszenie Tarczy Prywatności do czasu, gdy władze USA zastosują się do jej warunków, a zamiast tego zawsze preferowała „monitorowanie sytuacji" bez żadnych konkretnych rezultatów, jeśli chodzi o ochronę danych osób fizycznych i pewność prawa dla przedsiębiorstw; apeluje do Komisji, aby wyciągnęła wnioski z błędów popełnionych w przeszłości i odpowiadała na apele Parlamentu i ekspertów dotyczące przyjmowania i monitorowania przeszłych decyzji stwierdzających odpowiedni stopień ochrony oraz pozostawiła TSUE właściwe egzekwowanie unijnych przepisów o ochronie danych w związku ze skargami obywateli;

41. wzywa Komisję, aby ściśle monitorowała prawa i praktyki w zakresie ochrony danych w Zjednoczonym Królestwie, natychmiast informowała Parlament o wszelkich przyszłych zmianach w brytyjskim systemie ochrony danych i konsultowała się z Parlamentem w tej sprawie, a także przyznała Parlamentowi rolę kontrolną w nowych ramach instytucjonalnych, w tym w odniesieniu do właściwych organów, takich jak Specjalny Komitet ds. Współpracy Organów Ścigania i Wymiarów Sprawiedliwości;

o

o o

42. zobowiązuje swojego przewodniczącego do przekazania niniejszej rezolucji Komisji, państwom członkowskim i rządowi Zjednoczonego Królestwa.