Przegląd Prawniczy Uniwersytetu Warszawskiego
ISSN 1644-0242
Rok XVIII, nr 2/2019
DOI 10.26330/ppuw.2019.02.06

ORCID 0000-0003-1924-0402
*Maria Skwarcan**

Kontrola nad danymi o przelocie pasażera na tle problematyki praw podstawowych

1. Wprowadzenie

W sferze unijnej legislacji 2016 rok upłynął bez wątpienia pod znakiem reformy systemu ochrony danych osobowych. Obok szeroko dyskutowanego Rozporządzenia Ogólnego o Ochronie Danych Osobowych[1], Parlament Europejski i Rada przyjęły inne akty, o bardziej szczegółowym charakterze. Jednym z nich była przyjęta 27 kwietnia 2016 roku dyrektywa nr 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie oraz ich ścigania[2]. Choć sama idea przechowywania i przetwarzania danych pasażerów samolotu, w ramach walki z aktami terroryzmu i przestępczością zorganizowaną, pojawiła się na początku XXI wieku, pierwsze (i to nieskuteczne) próby uregulowania tej materii w ramach prawodawstwa Unii Europejskiej datuje się dopiero na rok 2007[3]. Niechęć instytucji i państw Unii Europejskiej oraz trudności związane z procesem legislacyjnym spowodowane były uprzedzeniem

* Uniwersytet Warszawski, Wydział Prawa i Administracji, ul. Krakowskie Przedmieście 26/28, 00-927 Warszawa, e-mail: me.smolny@student.uw.edu.pl.

[1] 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) (Dz.Urz. UE L 119/1 z 04.05.2016, s. 1).

[2] Dz.Urz. UE L 119/132 z 04.05.2016.

[3] Pomysł przyjęcia regulacji na poziomie unijnym, stwarzającej ramy dla systemu przechowywania i przetwarzania danych o przelocie pasażera dyskutowany był od 2007 roku, kiedy to Komisja zaproponowała Decyzję Ramową Rady w tej sprawie. Po wejściu w życie Traktatu Lizbońskiego, Komisja zastąpiła pomysł przyjęcia Decyzji Ramowej propozycją dyrektywy. Ostatecznie, proces legislacyjny został zablokowany działaniem parlamentarnej Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), która odrzuciła projekt w kwietniu 2013 roku.

do instrumentów masowej inwigilacji, które, zdaniem wielu, zbyt mocno ingerują oraz ograniczają ochronę danych osobowych i życie prywatne obywateli Unii Europejskiej. Ostateczny sukces zwolenników przyjęcia dyrektywy nie wynikał ze stopniowo dojrzewającej, przemyślanej decyzji politycznej, a raczej był rezultatem emocjonalnej reakcji na akty terroru, których europejskie państwa padły ofiarą w ostatnich latach.

Często takie raptowne decyzje, nieoparte na szerokiej akceptacji, stają się później źródłem kontrowersji i wątpliwości. Owa reguła znalazła swoje zastosowanie również w przypadku dyrektywy 2016/681. O braku pełnej aprobaty świadczy fakt, że jej implementacji nie dokonało w przewidzianym terminie w sumie 14 Państw Członkowskich[4], a rok po jej przyjęciu Trybunał Sprawiedliwości wydał opinię[5], co należy zaznaczyć – w innej sprawie, w której poddał restrykcyjnej ocenie umowę bilateralną zawartą między Unią Europejską a Kanadą, regulującą tę samą materię, a ponadto wskazał na pewien minimalny standard poszanowania prawa do prywatności i ochrony danych osobowych, których, jak się zdaje, również dyrektywa nie spełnia[6]. Niemniej jednak, pomimo szeregu kontrowersji, dyrektywa, jak i przyjęte na jej podstawie regulacje krajowe, a także umowy bilateralne w sprawie przekazywania danych o przelocie pasażera, zawarte między Unią Europejską a Stanami Zjednoczonymi[7] oraz Australią[8], wciąż obowiązują, i na co należy zwrócić uwagę, mają także swoich zwolenników na Starym Kontynencie. W rozważaniach nad

---

[4] Wśród państw, które przekroczyły graniczny termin implementacji, tj. 25 maja 2018 r. znalazły się: Austria, Bułgaria, Cypr, Republika Czeska, Estonia, Finlandia, Francja, Grecja, Luxemburg, Holandia, Portugalia, Rumunia, Słowenia and Hiszpania. W stosunku do nich Komisja Europejska wystosowała wezwanie do usunięcia uchybienia, zob. https://ec.europa.eu/commission/presscorner/detail/en/MEMO_18_4486, 26.04.2020.

[5] Zob. Opinia 1/15 TSUE z dnia 26 lipca 2017 r., ECLI:EU:C:2016:656.

[6] Trybunał m.in. ocenił, że pięcioletni okres przechowywania danych o przelocie pasażera jest niedopuszczalny. Szerzej w punkcie 3.1. niniejszego artykułu.

[7] Umowa między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, podpisana 14 grudnia 2011 r. (Dz.Urz. UE L 215 z dnia 11.08.2012).

[8] Umowa między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR), podpisana dnia 29 września 2011 r., (Dz.Urz. UE L 186 z 14.07.2012).

przedmiotowym instrumentem kontroli danych, obok prawa do prywatności i ochrony danych osobowych, na drugiej szali znajduje się bezpieczeństwo publiczne, stanowiące równie istotną wartość oraz cel interesu ogólnego Unii Europejskiej.

Wzmożona w ostatnich miesiącach dyskusja w materii przyszłego losu wspomnianych regulacji związana była z upływającym terminem obowiązywania umów łączących Unię Europejską z państwami trzecimi[9]. Jest to właściwy moment na chwilę refleksji nad różnicami w sposobie pojmowania i metody regulacji praw podstawowych w unijnym systemie prawnym oraz systemach państw trzecich, w szczególności Stanów Zjednoczonych, a także nad potrzebą, a nawet możliwością utrzymania obowiązujących regulacji w brzmieniu dotychczasowym w obliczu stanowczego stanowiska Trybunału Sprawiedliwości zawartego w Opinii 1/15.

Bez względu na ostateczny kierunek podjętych przez Unię Europejską w ostatnim czasie działań, problematyka przekazywania przez przewoźników lotniczych danych o przelocie pasażerów-obywateli państw członkowskich, wskazanym służbom państw trzecich, stanie się jeszcze bardziej relewantna z racji tego, że z każdym rokiem owa procedura kontroli dotyczy coraz większej liczby osób. Jak wskazują opublikowane przez Eurostat statystyki, w 2017 roku całkowita liczba pasażerów samolotów na terenie Unii Europejskiej wyniosła 1 043 mln, co stanowiło wzrost o 7.3% w porównaniu z rokiem 2016. Ponadto, aż 83% lotów, których pasażerami są obywatele UE to loty zagraniczne, realizowane wewnątrz Unii między Państwami Członkowskimi albo państwami trzecimi i Państwami Członkowskimi[10].

---

[9] Zgodnie z art. 26 ust.1 umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych oraz art. 26 ust. 1 umowy między Unią Europejską a Australią o przetwarzaniu i przekazywaniu przez przewoźników lotniczych australijskiej służbie celnej i granicznej danych dotyczących przelotu pasażera (danych PNR) okres obowiązywania umowy wynosi siedem lat od dnia jej wejścia w życie. Oznacza to, że obie umowy przestaną obowiązywać 1 sierpnia 2019 roku.

[10] Eurostat, *Air passenger transport – monthly statistics*, https://ec.europa.eu/eurostat/statistics-explained/pdfscache/9506.pdf, 25.04.2019.

2. Geneza i rozwój regulacji PNR

Niemal natychmiastową reakcją władz amerykańskich na tragiczne wydarzenia 11 września 2001 roku było powzięcie decyzji o konieczności prewencyjnego pozyskiwania danych pochodzących z *Passenger Name Record* (w skrócie danych PNR), czyli tytułowych danych o przelocie pasażera zawartych w imiennym rejestrze pasażera, a następnie poddania ich analizie, służącej wykryciu jednostek stanowiących zagrożenie terrorystyczne. Materialnym wyrazem tej decyzji był przyjęty już w listopadzie 2001 roku *Aviation and Transportation Security Act,* zobowiązujący przewoźników lotniczych, realizujących loty z i do Stanów Zjednoczonych, do udzielenia dostępu amerykańskim organom[11] do wewnętrznych zautomatyzowanych systemów rezerwacji, zawierających szereg danych, które to każdorazowo udostępniane są przez pasażerów przy zakupie biletów lotniczych.

Początkowy sceptycyzm Unii Europejskiej w stosunku do działań amerykańskiej legislacji, wyrażony ostrzeżeniem, że przepisy te mogą być sprzeczne z unijnymi regulacjami, chroniącymi dane osobowe obywateli Unii[12], ewoluował w podjęcie negocjacji, a następnie przyjęcie szeregu decyzji[13], zmierzających do zaaprobowania działań Stanów Zjednoczonych oraz włączenia się do nowego programu wykrywania i zapobiegania przestępstwom terrorystycznym. Z pewnością, bez inicjatywy oraz dużej presji ze strony dyplomacji amerykańskiej, Unia Europejska nie

---

[11] Organy amerykańskie mające dostęp do danych o przelocie pasażera to Biuro Celne i Ochrony Granic Stanów Zjednoczonych (United States Bureau of Customs and Border Protection) oraz Departament Bezpieczeństwa Wewnętrznego (DHS).

[12] J. Wojnowska-Radzińska, *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera – adekwatny środek do walki z terroryzmem i poważnymi przestępstwami czy forma masowej inwigilacji?*, Studia Europejskie, Nr 4 (84) 2017, s.165.

[13] Decyzja Komisji 2004/535/WE z dnia 14 maja 2004 r. w sprawie odpowiedniej ochrony danych osobowych zawartych w Passenger Name Record (PNR) pasażerów lotniczych przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych, Dz.Urz. UE L 232 z 6.07.2004; Decyzja Rady 2004/496/WE z dnia 17 maja 2004 r. w sprawie zawarcia Porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dot. nazwy rekordu pasażera (PNR) przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Biura Ceł i Ochrony Granic, Dz.Urz. UE L 183 z 20.05.2004.

podjęłaby działań, na które zdecydowała się w kolejnych latach[14] – a mianowicie, nie zawarłaby ze Stanami Zjednoczonymi umów o przekazywaniu i przetwarzaniu danych o przelocie pasażera (kolejno w 2007 i 2011 roku), podobnych porozumień z Australią (2011 roku) oraz Kanadą (2014 roku), a także nie przyjęłaby w kwietniu 2016 roku dyrektywy PE i Rady UE nr 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera. Pomimo wzmożonej aktywności Unii Europejskiej w dziedzinie kontroli danych PNR do dnia dzisiejszego nie milkną głosy sprzeciwu wśród niektórych eurodeputowanych oraz europejskich organizacji pozarządowych, które wskazują na potrzebę ograniczenia tychże działań na rzecz zwiększenia gwarancji ochrony praw zawartych w art. 7 i 8 Karty Praw Podstawowych – prawa do poszanowania życia prywatnego oraz ochrony danych osobowych. Poniekąd, owa krytyka przyniosła owoce w postaci odrzucenia przez Parlament Europejski w 2013 roku projektu dyrektywy regulującej przetwarzanie danych PNR[15], który został negatywnie zaopiniowany przez szereg podmiotów– Europejski Komitet Ekonomiczno-Społeczny, Agencję Praw Podstawowych Unii Europejskiej oraz Europejskiego Inspektora Ochrony Danych[16]. Powrót sceptycznych nastrojów w Unii przyniósł plony także w kolejnych latach. W związku z nowo obranym kierunkiem, umowa z Kanadą zawarta w 2014 roku wzbudziła na tyle duże wątpliwości, że Parlament Europejski zdecydował się je rozwiać, kierując do Trybunału Sprawiedliwości wniosek o wydanie opinii w sprawach zgodności projektowanej umowy z Kartą Praw Podstawowych oraz odpowiedniej dla niej podstawy prawnej. Wydana 26 lipca 2017 roku Opinia 1/15 TSUE jednoznacznie przekreśliła możliwość zawarcia umowy z Kanadą w dotychczasowej postaci, uznając jej postanowienia za godzące w prawa chronione Kartą. Dziwić

[14] D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?*, ICLR, No. 1/2017, s. 879.

[15] Projekt dyrektywy odrzuciła Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), która zarzuciła m.in. niespełnienie zasad proporcjonalności i konieczności.

[16] Zob. Opinia Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 5 maja 2011 r., Dz.Urz. UE C 218 z 23.7.2011; Opinia Europejskiego Inspektora Ochrony Danych z dnia 25 marca 2011 r., Dz.Urz. UE C 181 z 22.6.2011; Opinia Agencji Praw Podstawowych Unii Europejskiej z dnia 14 czerwca 2011 r., (COM(2011) 32 wersja ostateczna), dostępna pod adresem https://fra.europa.eu/sites/default/files/fra_uploads/1786-FRA-PNR-Opinion-2011_EN.pdf, 26.04.2020.

zatem może fakt, że rok wcześniej, pomimo przeciwnych tendencji, do przyjęcia dyrektywy w sprawie wykorzystywania danych dotyczących przelotu pasażera ostatecznie doszło. Tak jak w 2001 roku motorem podjęcia zdecydowanych kroków legislacyjnych były zamachy na *World Trade Centre*, tak dyrektywa z 2016 roku była bezpośrednią reakcją na tragiczne w skutkach wydarzenia do jakich doszło w Paryżu w styczniu i listopadzie 2015 roku, których symbolem pozostanie atak terrorystyczny na redakcję tygodnika satyrycznego *Charlie Hebdo*.

3. Dane wchodzące w zakres imiennego rejestru pasażera

Podstawowym źródłem kontrowersji pozostaje definicja danych PNR. Zgodnie ze słowniczkiem pojęć, zawartym w dyrektywie 2016/681 oznaczają one „zbiór danych o podróży każdego pasażera, który zawiera informacje niezbędne, aby umożliwić przetwarzanie i weryfikowanie rezerwacji przez przewoźników lotniczych obsługujących rezerwację i lot w odniesieniu do każdego przelotu zarezerwowanego przez jakąkolwiek osobę lub w jej imieniu, bez względu na to, czy zbiór ten znajduje się w systemach rezerwacji, systemach odpraw pasażerskich lub równorzędnych systemach pełniących te same funkcje". Zastrzeżenia związane z definicją danych PNR skupiają się wokół powszechnego charakteru ich przetwarzania. Każdorazowo, przy rezerwacji podróży, dane wszystkich pasażerów poddane są weryfikacji. Zdaniem przeciwników dyrektywy, owo rozwiązanie inwigilacji jednostek, co do których nie ma wstępnych podejrzeń, nie jest uzasadnione[17]. Powszechnie uznaje się jednak, że system kontroli danych PNR ma charakter prewencyjny, w związku z czym jego skuteczność oraz celowość zagwarantowana jest tylko w warunkach nieograniczonego podmiotowo dostępu do danych osobowych. Ten element odróżnia właśnie dane PNR od tzw. *Advanced Passenger Information* (API), czyli zaawansowanych informacji o pasażerach, obejmujących dane paszportowe, a zatem imię i nazwisko, datę urodzenia, numer dokumentu tożsamości oraz narodowość. Podczas gdy druga z wymienionych kate-

[17] D. Bigo [i in.], *The EU Counter-Terrorism Policy Responses to the Attacks in Paris: Towards an EU Security and Liberty Agenda*, CEPS, Nr 81, 2015, s. 12–14.

gorii danych może służyć identyfikacji znanych terrorystów i przestępców poprzez zastosowanie systemów ostrzegania, dane PNR pozwalają na ocenę ryzyka ze strony dotychczas nieznanych służbom jednostek[18].

Dane, które bierze się przy takiej ocenie pod uwagę są szczegółowo określone w Załączniku I zarówno w przypadku dyrektywy, jak i umów bilateralnych. Poza elementami wykazu niewywołującymi większych kontrowersji, a dotyczącymi daty, trasy, biura podróży oraz zajmowanego miejsca i bagażu, spore wątpliwości wzbudzają natomiast niedookreślone kategorie informacji, przede wszystkim tzw. „Uwagi ogólne", w zakres których wchodzą dodatkowe prośby pasażera, m.in. o wózek inwalidzki albo preferowany posiłek, który może stanowić wskazówkę co do jego pochodzenia oraz wyznawanej religii. Jest to o tyle problematyczne, że na mocy motywu 15 dyrektywy, artykułu 8 umowy PNR zawartej z Australią oraz artykułu 6 umowy ze Stanami Zjednoczonymi[19] z wykazu danych PNR zostały wyłączone dane szczególnie chronione, takie jak: religia, rasa, pochodzenie etniczne, czy też poglądy polityczne, stan zdrowia, życie i orientacja seksualna pasażera. Pomimo istnienia gwarancji w postaci przedstawionego zakazu, *de facto* ochrona danych wrażliwych jest w dużej mierze ograniczona, co stanowi rezultat braku pełnej precyzji przy redakcji załącznika.

4. Problematyka PNR na tle wybranych regulacji unijnych

4.1. Problem zgodności postanowień dyrektywy 2016/681 i bilateralnych umów PNR z Kartą Praw Podstawowych

Spór co do (nie)zgodności regulacji PNR z prawami podstawowymi nie osadza się jedynie na treści i redakcji wykazu zatrzymywanych oraz przetwarzanych danych o przelocie pasażera, a obejmuje szereg innych

[18] EP Research Service, *Briefing: The proposed EU passenger name records (PNR) directive,* http://www.europarl.europa.eu/EPRS/EPRS-Briefing-554215-The-EU-PNR-Proposal-FINAL.pdf, s. 2, 20.04.2019.

[19] Wyłączenie przetwarzania danych szczególnie chronionych w przypadku dyrektywy i umowy z Australią jest pełne, natomiast zgodnie z art. 6 umowy PNR ze Stanami Zjednoczonymi, wobec tego rodzaju danych stosuje się zautomatyzowane systemy filtrujące i maskujące, a ponadto od zakazu ich dalszego przetwarzania przez służby amerykańskie istnieją przewidziane w umowie wyjątki.

uwag. Mimo to, nieścisłość załączników umowy i dyrektywy stanowi podstawowy zarzut z racji tego, że stwarza zagrożenie dla bezpieczeństwa danych szczególnie chronionych, a w konsekwencji godzić może w artykuł 7 Karty Praw Podstawowych[20] (prawo do poszanowania życia prywatnego i rodzinnego) oraz artykuł 21 KPP (zakaz dyskryminacji), przyjmując przy tym formę nawet bezpośredniej dyskryminacji w sytuacji weryfikacji pasażerów w oparciu o dane na temat preferowanego posiłku albo informację o niepełnosprawności pasażera[21]. Wiele kontrowersji wzbudza również zgodność dyrektywy 2016/681 oraz umów bilateralnych z artykułem 8 KPP, poświęconym prawu do ochrony danych osobowych. W tym kontekście wątpliwości budzi dopuszczalny okres przechowywania danych – wynoszący pięć lat w przypadku postanowień dyrektywy (art. 12), pięć i pół roku w sytuacji przekazania danych organom australijskim (art. 16), oraz piętnaście lat w przypadku umowy ze Stanami Zjednoczonymi (art. 8), a także, po upływie tego okresu, możliwość łatwego przywrócenia danych do bazy.

Krytyczne stanowisko Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych , które skutkowało fiaskiem pierwszej propozycji dyrektywy w 2013 roku, oparte było na zarzucie ingerencji dyrektywy w prawo swobodnego przepływu osób[22]. Zgodnie z unijną dyrektywą 2004/38/WE[23], regulującą tę kwestię, Państwa Członkowskie mogą ograniczyć swobodę przemieszczania się obywateli Unii Europejskiej ze względu na bezpieczeństwo publiczne albo porządek publiczny.

---

[20] Karta Praw Podstawowych Unii Europejskiej z dnia 7 grudnia 2000 r., Dz.Urz. UE 2016 C 202, s.1.

[21] Opinia Agencji Praw Podstawowych Unii Europejskiej z dnia 14 czerwca 2011 r. (COM(2011) 32 final) s. 7–8.

[22] Zob. Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych, Sprawozdanie w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych dotyczących przelotu pasażera w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania, COM(2011) 0032 – C7-0039/2011 – 2011/0023(COD) z dnia 23.04.2013 r.

[23] Dyrektywa 2004/38/WE Parlamentu Europejskiego i Rady z dnia 29 kwietnia 2004 r. w sprawie prawa obywateli Unii i członków ich rodzin do swobodnego przemieszczania się i pobytu na terytorium Państw Członkowskich, zmieniająca rozporządzenie (EWG) nr 1612/68 i uchylająca dyrektywy 64/221/EWG, 68/360/EWG, 72/194/EWG, 73/148/EWG, 75/34/EWG, 75/35/EWG, 90/364/EWG, 90/365/EWG i 93/96/EWG (Dz.Urz. UE L 158, 30.4.2004, s. 77–123).

Jednakowoż, takie działania muszą pozostawać zgodne z zasadą proporcjonalności, a ponadto opierać się na wyłącznej przesłance osobistego zachowania jednostki, stanowiącego rzeczywiste, aktualne i wystarczająco poważne zagrożenie dla jednego z podstawowych interesów społecznych. Ryzyko naruszenia tej zasady przedstawiciele Parlamentu Europejskiego dopatrzyli się w, projektowanym w dyrektywie, rozszerzeniu systemu kontroli danych PNR o loty realizowane między Państwami Członkowskimi Unii Europejskiej. Ostatecznie członkowie Komisji LIBE powzięli wątpliwość, czy tak szeroko zakrojony system kontroli danych jest w rzeczy samej niezbędnym narzędziem, służącym efektywnemu przeciwdziałaniu przestępczości i terroryzmowi.

Dowody efektywności systemów kontroli danych o przelocie pasażera wydają się być kluczowe dla udowodnienia konieczności formowania tego systemu na poziomie unijnym. Podczas gdy Komisja Europejska przyznaje, że stosowne, szczegółowe statystyki w tym zakresie nie są dostępne, wskazuje na wyrywkowe informacje uzyskane od poszczególnych państw, które mają dowodzić, że przetwarzanie danych PNR doprowadziło do „przełomowego postępu" w walce przeciwko terroryzmowi, przemytowi narkotyków i handlu ludźmi. Na poparcie swojego stanowiska Komisja przedstawiła dane dotyczące liczby przechwycenia narkotyków przez służby w Belgii, Szwecji i Wielkiej Brytanii[24]. Niemniej jednak, twierdzenia podniesione przez Komisję zostały powszechnie skrytykowane za swoją niespójność oraz anegdotyczną, fragmentaryczną i tym samym niedostateczną naturę[25].

Ponadto, aby uznać system kontroli danych PNR za konieczny, w pierwszej kolejności należałoby stwierdzić, że istniejące środki, do których na poziomie unijnym zalicza się dyrektywę w sprawie API[26] (zaawansowanej informacji o pasażerach), wizowy system informacyjny, a także system Schengen, są niewystarczające. Dotychczas do takiej oceny

[24] Zob. Komunikat Komisji Europejskiej w sprawie kompleksowego podejścia do ochrony danych osobowych w Unii Europejskiej, COM(2010) 609 final, Bruksela, 4.11.2010.

[25] E. Brouwer, *Ignoring Dissent and Legality: The EU's proposal to share the personal information of all passengers*, CEPS, 2011, s. 2–3.

[26] Dyrektywa Rady 2004/82/WE z dnia 29 kwietnia 2004 r. w sprawie zobowiązania przewoźników do przekazywania danych pasażerów, Dz.Urz. UE L 261 z 6.08.2004, s. 24–27.

nie doszło, nie zaproponowano też mniej inwazyjnych, alternatywnych narzędzi.

Jak zauważono, kluczowe znaczenie w dyskusji nad zgodnością dyrektywy z prawem unijnym ma także zasada proporcjonalności, wyrażona w art. 52 Karty Praw Podstawowych, której zachowanie niezbędne jest za każdym razem, gdy dochodzi do ograniczenia praw i wolności uznanych przez Kartę. Wymóg ten może być trudny do spełnienia, biorąc pod uwagę szeroki zakres podmiotowy dyrektywy (weryfikacji poddane są dane wszystkich pasażerów lotów międzynarodowych, a także, jeśli państwa implementujące dyrektywę się na to zdecydowały, lotów wewnątrzunijnych, między Państwami Członkowskimi). Proporcjonalność takich działań zależy, zdaniem niektórych, od ich tymczasowego charakteru oraz bezpośredniego związku z określonym, zidentyfikowanym zagrożeniem, co oczywiście nie jest spójne z ideą przede wszystkim prewencyjnego, a w mniejszym stopniu represyjnego, powszechnego systemu kontroli danych, jakim jest system PNR[27].

Do wyżej przedstawionych argumentów krytycznych przyłączają się także organizacje pozarządowe[28], zdaniem których dyrektywa 2016/681 stanowi inwazyjny środek kontroli i kolejny krok w kierunku formowania społeczeństwa poddanego stałej inwigilacji.

4.2. Zarzuty Trybunału Sprawiedliwości zawarte w Opinii 1/15

Wydana w lipcu 2017 r. Opinia w sprawie zgodności umowy PNR zawartej z Kanadą z prawem unijnym, była kluczowym i historycznym wydarzeniem. Historycznym z tego względu, że po raz pierwszy Trybunał analizował zgodność umowy międzynarodowej z postanowieniami Karty Praw Podstawowej. Kluczowym, ponieważ ostatecznie ugruntowała

[27] Opinia 10/2011 Grupy Roboczej ds. ochrony danych utworzonej na mocy art. 29 z 5.04.2011, s. 4–5.

[28] Do grona przeciwników dyrektywy należy stowarzyszenie European Digital Rights oraz organizacja Statewatch, a także polska Fundacja Panoptykon. Zob. M. Hynes, analiza Statewatch, *Proposal for a Directive on the use of Passenger Name Record data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime*, 2011, s. 6–8.

kierunek, jaki wyznacza orzecznictwo Trybunału – kierunek wysokiej ochrony praw podstawowych gwarantowanych w Karcie[29].

Parlament Europejski w swoim wniosku zawarł dwa pytania: pierwsze dotyczące zgodności umowy z postanowieniami traktatów i Kartą praw podstawowych Unii Europejskiej w zakresie prawa osób fizycznych do ochrony danych osobowych oraz drugie o właściwą podstawę prawną zawarcia takiej umowy.

W odpowiedzi na wniosek Parlamentu Trybunał jednoznacznie stwierdził, że przewidywana umowa nie może zostać zawarta w obecnej postaci z powodu jej niezgodności z art. 7, 8, 21 Karty Praw Podstawowych. Wskazał na nieścisłości w załączniku I w punktach: 5 [„dostępne informacje dotyczące programów dla stałych klientów (*frequent flier*) i dotyczące korzyści (np. darmowe bilety, zamiana klasy biletu na wyższą itd.)]", 7 [wszelkie dostępne informacje kontaktowe (w tym informacje na temat jednostki, która stworzyła dane] oraz 17 [„uwagi ogólne w tym: inne informacje dodatkowe (OSI) oraz informacje o usługach specjalnych (SSI) i o prośbach o usługi specjalne (SSR)"], które dopuszczają poddanie weryfikacji i przechowywaniu danych szczególnie chronionych. Jak Trybunał zaznaczył, przekazywanie do Kanady tego rodzaju danych wymagałoby precyzyjnego i szczególnie solidnego uzasadnienia, wywodzonego z innych powodów niż ochrona bezpieczeństwa publicznego przed terroryzmem i poważną przestępczością międzynarodową.

Ponadto, uznał oznaczony w umowie, pięcioletni okres przechowywania danych za zbyt długi oraz stwierdził, że umowa jest zgodna z postanowieniami Karty i Traktatów jedynie, gdy gwarantuje, że nadzór nad przestrzeganiem norm odnoszących się do ochrony pasażerów lotniczych w zakresie przetwarzania ich danych PNR będzie sprawowany przez niezależny organ kontroli, czego umowa z Kanadą nie przewiduje[30].

---

[29] Opinia 1/15 jest swoistym podsumowaniem wyroków TSUE wydanych w ostatnich latach. Rzecznik Generalny Paolo Mengozzi przyznał, że Trybunał wydając opinię oparł się na tezach wyroków w sprawach łączonych *Digital Rights C-293/12 i C-594/12* oraz *Schrems* C-362/14.

[30] Trybunał ponadto stwierdził, że o ile cel umowy PNR (zapewnienie bezpieczeństwa publicznego) stanowi „cel interesu ogólnego UE, który może uzasadniać ingerencje, nawet poważne, w prawa podstawowe ustanowione w art. 7 i 8 KPP", to zakres tej ingerencji musi być uzasadniony i mieć charakter konieczny, których to warunków umowa z Kanadą nie spełnia.

Co ciekawe i istotne z perspektywy rozważań nad przyszłością obowiązujących umów bilateralnych – ze Stanami Zjednoczonymi oraz Australią, wszystkie postanowienia, na których niezgodność z prawem Unii Europejskiej zwrócił uwagę Trybunał, mają podobne brzmienie w owych umowach, obowiązujących do sierpnia 2019 roku. Co więcej, w wielu przypadkach zostały sformułowane w taki sposób, że gwarantują jeszcze niższy poziom ochrony praw podstawowych. Przykładem takiego postanowienia jest artykuł 8 Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, regulujący okres przechowywania danych[31]. Przy uwzględnieniu wszelkich wyjątkowych sytuacji przewidzianych w tej jednostce redakcyjnej, okres retencji danych może wynieść nawet piętnaście lat.

Podobnie, z racji przyjęcia dyrektywy PNR na rok przed wydaniem opinii przez Trybunał Sprawiedliwości, szereg postanowień unijnej regulacji również nie jest kompatybilna ze standardem wskazanym przez Trybunał. Oprócz pięcioletniej retencji danych, załącznik I dyrektywy 2016/681 zawiera elementy wykazu danych, takie jak „Uwagi ogólne", które zostały uznane przez Trybunał za godzące w prawa do prywatności i ochrony danych osobowych oraz w zakaz niedyskryminacji.

5. Kontradyktoryjne koncepcje prywatności: Stany Zjednoczone a Unia Europejska

Podsumowując zarzuty Trybunału, innych instytucji i organów Unii Europejskiej, a także organizacji pozarządowych i krytycznie nastawionych do kontroli danych PNR Europejczyków należy stwierdzić, że niemal wszystkie dotyczą zagrożenia naruszenia praw podstawowych – w szczególności prawa do prywatności i wywodzącej się z niego ochrony danych osobowych jednostek.

[31] Art. 8 Umowy USA-UE: „1. DHS przechowuje dane PNR w aktywnej bazie danych przez okres nieprzekraczający pięciu lat. (...) 3. Po upływie okresu przechowywania w bazie aktywnej dane PNR przenoszone są do archiwalnej bazy danych na okres nieprzekraczający dziesięciu lat. (...)".

Ze względu na fakt, że to Stany Zjednoczone jako pierwsze uregulowały kwestię przetwarzania danych PNR i lobbowały przyjęcie podobnych przepisów przez Unię Europejską zasadne jest poddanie analizie stosunku obu podmiotów do ochrony prywatności.

Bezsprzecznie, ochrona sfery życia prywatnego jako fundamentalne prawo stanowi globalne wyzwanie, z którym mierzą się wszystkie demokratyczne państwa świata. Niemniej, koncepcja samego prawa do prywatności oraz metod stwarzania odpowiednich warunków dla jego realizacji, w zależności od państwa, znacząco się różni. Najlepszym tego dowodem jest odmienny stosunek Stanów Zjednoczonych i Unii Europejskiej do umów i aktów prawnych przyjmowanych w sprawie przekazywania i przetwarzania danych o przelocie pasażera. Podczas gdy na Starym Kontynencie podnoszone są argumenty zbyt dużej ingerencji regulacji w życie prywatne jednostek, po drugiej stronie Oceanu Atlantyckiego nikt nie ma wątpliwości, że imperatyw bezpieczeństwa publicznego jest wystarczającym uzasadnieniem przyjęcia instrumentów masowej i kompleksowej kontroli danych osobowych[32]. W związku z istniejącym dysonansem, partnerzy, chcąc uniknąć nieporozumień, zmuszeni są stale prowadzić rozmowy oraz negocjacje, które stanowią szansę artykułowania własnych priorytetów i wartości oraz służą lepszemu zrozumieniu drugiej strony.

I tak, przedstawiciele europejskich systemów prawnych zarzucają stronie amerykańskiej, że w porównaniu z międzynarodowymi standardami ochrony prywatności, państwo to przyjmuje w tym zakresie bardzo luźną, liberalną postawę tzw. *laissez faire*[33]. Nieznane systemom europejskim jedynie wąskie, ściśle określone gwarancje poszanowania prawa do prywatności, (m.in. w stosunku do rejestrów medycznych) opiera się na założeniu, że co do zasady sfera przetwarzania danych osobowych pozostaje nieuregulowana, niepoddana żadnym ograniczeniom normatywnym.

---

[32] A. Rizer, *Dog Fight: Did The International Battle Over Airline Passenger Name Records Enable The Christmas-day Bomber?*, CULR, No. 1/2010, s. 79.

[33] Tamże, s. 81.

Na przeciwległym biegunie znajduje się natomiast Unia Europejska, która realizuje wizję silnych gwarancji prawa do prywatności i poważnie traktuje wszelkie próby ingerencji i jego ograniczania. W konsekwencji wiele państw członkowskich Unii Europejskiej znowelizowało na przestrzeni lat swoje konstytucje, gwarantując w nich jednostkom *expressis verbis* ochronę życia prywatnego. Dodatkowo, w ramach Wspólnoty przeprowadzono systemową reformę ochrony danych osobowych, przyjmując generalne rozporządzenie regulujące kompleksowo kwestię przetwarzania tychże danych. Z pewnością rozwiązanie stosowane przez prawodawcę unijnego jest znacznie bardziej przejrzyste od fragmentarycznych regulacji amerykańskich. Z drugiej zaś strony, sektorowe podejście Stanów Zjednoczonych jest bardziej elastyczne, pozwalające rynkowi samemu regulować potrzebę zwiększenia albo zmniejszenia gwarancji dla ochrony prywatności, w związku z czym władza publiczna ogranicza do minimum aktywność prawodawczą w tej materii.

Podstawowym źródłem znaczących różnic w postrzeganiu ochrony życia prywatnego są ustawy zasadnicze – Konstytucja Stanów Zjednoczonych oraz konstytucje państw Unii Europejskiej. Z racji, że pierwsza poprawka do Konstytucji gwarantuje prawo swobodnej wypowiedzi, także na temat innych ludzi i to bez ograniczeń w stosunku do wypowiedzi naruszającej prawo do prywatności, paradoksalnie amerykańska ustawa zasadnicza chroni bardziej otwarcie potencjalnego naruszyciela prawa do prywatności niż ofiary naruszeń prawa do prywatności[34]. Co więcej, interesującą obserwacją jest dostrzeżenie, że ani w Konstytucji, ani w Deklaracji Niepodległości nie występuje słowo „prywatność" lub jego ekwiwalent. Przeciwne rozwiązania prezentują konstytucje państw Europy. Na Starym Kontynencie dominuje pogląd, że ochrona prywatności na poziomie konstytucyjnym odzwierciedla wagę i akcentuje fundamentalny charakter prawa do prywatności. W europejskich systemach prawnych to rządy państw są zobowiązane przestrzegać i chronić prawo jednostek do życia prywatnego i rodzinnego oraz stwarzać wystarczające warunki dla jego poszanowania. System amerykański co do zasady pozostawia natomiast jednostkom

[34] T.L. Forsheit, *Privacy, Data Security and Outsourcing*, 946 PLI/PAT 11, 17, 2008.

podejmowanie działań, mających na celu ochronę informacji na temat ich życia osobistego.

Powyższa analiza ukazuje olbrzymie różnice w postrzeganiu problematyki praw podstawowych – prawa do poszanowania życia prywatnego i ochrony danych osobistych między Stanami Zjednoczonymi a Unią Europejską. Od czasu do czasu słychać jednak głosy, że różnice te stopniowo się zacierają i mają coraz mniejsze znaczenie, czego przykładem są słowa byłego Sekretarza Bezpieczeństwa Krajowego Stanów Zjednoczonych, Michaela Chertoff'a, który stwierdził, że choć różnice w nastawieniu do systemu wymiany danych PNR istnieją, ich znaczenie zdecydowanie się przecenia, natomiast coraz wyraźniejszą tendencją jest zjawisko konwergencji między państwami, zwłaszcza między transatlantyckimi partnerami, których łączy idea walki z terroryzmem[35].

Niedawna Opinia TSUE 1/15 może jednak świadczyć o utrzymaniu europejskiego, historycznie ukształtowanego standardu wysokiej ochrony praw podstawowych, do zniesienia którego nie jest wystarczające uzasadnienie w postaci ochrony bezpieczeństwa publicznego przed terroryzmem i poważną przestępczością międzynarodową.

6. Wnioski

W sierpniu 2019 roku doszło do automatycznego przedłużenia terminu obowiązywania umów między Unią Europejską a państwami trzecimi – Australią i Stanami Zjednoczonymi, o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera. Pomimo tego, że niecałe dwa lata temu Trybunał Sprawiedliwości uznał podobną w treści umowę zawartą z Kanadą za niezgodną z Traktatami i Kartą Praw Podstawowych, losy dwóch pierwszych umów były, są i zapewne będą odmienne. Pomimo szeroko dyskutowanych na kontynencie europejskim kontrowersji związanych z systemem PNR, zarówno ze strony amerykańskich, jak i unijnych przedstawicieli dostrzec można wolę polityczną kontynuowania dotychczasowej współpracy. Potwierdzeniem tego było wydane 9 listopada 2018 roku, wspólne oświadczenie,

[35] A. Rizer, *Dog*..., s. 94.

wieńczące unijno-amerykańskie spotkanie na szczeblu ministerialnym[36]. Jest to z pewnością konsekwencja wzmożonego w ostatnich latach zagrożenia terrorystycznego w Europie, które ukazało potrzebę zastosowania odpowiednich środków zapobiegawczych, także w postaci zacieśnionej współpracy między organami ścigania poszczególnych państw. Kierowane tą samą potrzebą, instytucje Unii Europejskiej ostatecznie osiągnęły konsensus w sprawie uregulowania materii przechowywania i przetwarzania danych PNR w formie dyrektywy. Po dniu 27 kwietnia 2016 roku, w którym to Parlament Europejski i Rada przyjęły dyrektywę 2016/681, głosy krytyczne jednak nie umilkły, a z pewnością nasiliły się po wydaniu w lipcu 2017 roku Opinii 1/15 TSUE, bardzo wysoko stawiającej poprzeczkę odpowiedniego standardu ochrony praw podstawowych. Odmienne kierunki działań instytucji unijnych wskazują, że niezwykle trudno jest osiągnąć właściwą równowagę między zwalczaniem terroryzmu i poważnej przestępczości a ochroną danych osobowych, przy jednoczesnym poszanowaniu prywatności osób, których dane dotyczą. Niemniej jednak, przez wzgląd na wciąż aktualne, podwyższone zagrożenie terrorystyczne spodziewać można się w najbliższych latach aktywności Unii Europejskiej na rzecz utrzymania systemu kontroli danych o przelocie pasażera oraz zacieśnieniu współpracy w tym zakresie z państwami trzecimi.

[36] Joint EU-U.S. statement following the EU-U.S. Justice and Home Affairs Ministerial Meeting, https://www.consilium.europa.eu/en/press/press-releases/2018/11/09/joint-eu-u-s-statement-following-the-eu-u-s-justice-and-home-affairs-ministerial-meeting/, 27.04.2019.

S t r e s z c z e n i e

W dobie walki ze zjawiskami terroryzmu i przestępczości zorganizowanej, Unia Europejska we współpracy z państwami trzecimi podejmuje szereg działań prewencyjnych, w tym takie, które zakładają kontrolę osób fizycznych poprzez analizę ich danych osobowych. Jednocześnie prawo do ochrony tych danych oraz ściśle powiązane z nim prawo do poszanowania życia prywatnego i rodzinnego należą do katalogu praw chronionych Kartą Praw Podstawowych. Przekazywanie danych osobowych do państw trzecich wiąże się zatem z ryzykiem naruszenia pewnej sfery wolności i fundamentalnych praw jednostek. Dążąc do utrzymania odpowiedniego standardu ochrony danych, w kwietniu 2016 roku przyjęto dyrektywę 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera w celu m.in. wykrywania i zapobiegania przestępstwom terrorystycznym. Regulacja ta, podobnie jak umowy bilateralne, pozwalające europejskim przewoźnikom przekazywać dane pasażera państwom trzecim, mogą wzbudzać pewne wątpliwości, zwłaszcza na kontynencie europejskim, hołdującym ścisłej ochronie prawa do prywatności.

Słowa kluczowe: prawa podstawowe, dane PNR, prawo do poszanowania życia prywatnego, ochrona danych osobowych, dyrektywa nr 2016/681

Control over Passenger Name Record data in relation to fundamental rights concerns

S u m m a r y

In the era of global battle against phenomena of terrorism and organized crime, the EU in cooperation with third countries undertakes preventive actions, including those which involve control over individuals through an analysis of their personal data. At the same time, the right to personal data protection and, tightly bound to it, right to privacy are included and protected by the Charter of Fundamental Rights. Therefore, a transfer of citizens' personal data to third countries involves a risk of liberties and individual rights' violation. Striving to maintain an accurate standard of data protection, in April 2016, the European Parliament and Council adopted a directive 2016/681 on the use of passenger name record (PNR) data. The regulation, similarly as bilateral agreements, enabling European air carriers to transfer passenger data to the United States and Australia, cause some controversies, especially on the European continent, which is known for its sensitivity to the right to privacy.

Keywords: fundamental rights, PNR data, right to privacy, data protection, directive no. 2016/681

Maria Skwarcan
University of Warsaw, Faculty of Law and Administration,
ul. Krakowskie Przedmieście 26/28, 00–927 Warszawa, Poland,
e-mail: me.smolny@student.uw.edu.pl.