*Julia 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?

Wprowadzenie

W dniu 24 maja 2016 r. weszła w życie dyrektywa nr 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR)[1] w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie oraz ich ścigania[2]. Jak podkreślił poseł sprawozdawca Timothy Kirkhope, Unia przyjęła „ważny nowy instrument do walki z terrorystami i przemytnikami. Dzięki zbieraniu, udostępnianiu i analizowaniu danych PNR nasze agencje wywiadowcze będą mogły zidentyfikować wzorce sposobów zachowania budzących podejrzenia, na które należy zwracać uwagę. PNR nie jest panaceum, ale państwa, które mają krajowe systemy, wielokrotnie dowiodły ich skuteczności"[3]. Przedmiotowa dyrektywa reguluje przekazywanie przez przewoźników lotniczych danych dotyczących przelotu pasażerów lotów międzynarodowych z i do państw członkowskich, jak również przetwarzanie tych danych i ich wymianę zarówno między państwami członkowskimi, jak i z państwami trzecimi.

* **Dr Julia Wojnowska-Radzińska** – Katedra Prawa Konstytucyjnego Uniwersytetu im. Adama Mickiewicza w Poznaniu, e-mail: juliaw@amu.edu.pl.

[1] Termin PNR pochodzi z ang. *Passenger Name Record*.

[2] Dz. Urz. UE L 119/132 z 04.05.2016 r. (dalej jako: dyrektywa 2016/681, dyrektywa).

[3] Fragment wypowiedzi posła sprawozdawcy T. Kirkhope'a (ECR, UK) pochodzi ze strony internetowej: http://www.europarl.europa.eu/news/pl/press-room/20160407IPR21775/parlament-przyjal-dyrektywe-w-sprawie-danych-pasazerow-linii-lotniczych-pnr (dostęp 6.06.2017).

Warto zauważyć, że prace legislacyjne nad omawianą dyrektywą trwały ponad sześć lat, co dowodzi złożoności przedmiotowej problematyki, która odnosi się do kwestii właściwej równowagi, jaką należy osiągnąć między, z jednej strony, koniecznością ochrony przez państwo zasadniczych interesów jego bezpieczeństwa (w szczególności związanych z zagrożeniem stwarzanym przez terroryzm), a z drugiej strony – zagwarantowaniem jednostce poszanowania jej podstawowych praw. Głównym założeniem dyrektywy 2016/681 jest harmonizacja przepisów państw członkowskich UE dotyczących ochrony danych, aby umożliwić wykorzystanie danych PNR w walce z terroryzmem i poważną przestępczością. Zgodnie z art. 18 ust. 2 dyrektywy państwa członkowskie są zobowiązane do transpozycji niniejszej dyrektywy do dnia 28 maja 2018 r.[4] Niniejszy artykuł ma na celu analizę przepisów dyrektywy 2016/681 w zakresie przetwarzania danych PNR z punktu widzenia wymogów zasady proporcjonalności, z uwzględnieniem najnowszego orzecznictwa Trybunału Sprawiedliwości UE (TSUE) w zakresie dopuszczalnych ograniczeń prawa do prywatności i ochrony danych osobowych.

Geneza dyrektywy 2016/681

Zamachy z 11 września 2001 r. na World Trade Center w Nowym Jorku bez wątpienia miały decydujący wpływ na podjęcie działań legislacyjnych w celu uregulowania gromadzenia i przetwarzania danych PNR na szczeblu UE[5]. Wydarzenia te uświadomiły organom ścigania w Stanach Zjednoczonych i krajach europejskich, że gromadzenie i analizowanie danych PNR może ułatwić wykrywanie osób stanowiących zagrożenie terrorystyczne. W ich efekcie Stany Zjednoczone przyjęły jeszcze w tym samym roku przepisy *Aviation and TransportationSecurity Act*, zobowiązujące przewoźników lotniczych wykonujących przeloty na trasach do i ze Stanów Zjednoczonych do udzielania dostępu elektronicznego dla Biura Celnego i Ochrony Granic Stanów Zjednoczonych (*United States Bureau of Customs and Border Protection* – CBP) oraz Departamentu Bezpieczeństwa Wewnętrznego (DHS) do danych zawartych w ich zautomatyzowanych systemach rezerwacji i kontroli odlotów, zwanych „imiennym rejestrem pasażera" (*Passenger Name Record* – PNR)[6]. Dane dotyczące

[4] Art. 18 ust. 2 dyrektywy 2016/681.

[5] D. Lowe, *The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?*, "International Criminal Law Review", No. 1/2017, s. 80. Zob. także: C. Blasi Casagran, *The Future EU PNR System: Will Passenger Data be Protected?*, "European Journal of Crime, Criminal Law and Criminal Justice", No. 3/2015, s. 241–257.

[6] Ibidem. Zob. także: C. Kaunert, S. Leonard, A. McKenzie, *The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT*, "European Security", No. 4/2012, s. 483; P. De Hert, V. Papakon-

przelotu pasażerów (PNR) to informacje dostarczane przez pasażerów przy rezerwacji lotu i odprawie. Zawierają one szereg informacji, takich jak: daty podróży, trasa podróży, informacje o bilecie, dane kontaktowe, biuro podróży, w którym zarezerwowano bilet, użyte środki płatności, preferencje co do posiłków, numer miejsca oraz informacje o bagażu.

W czerwcu 2002 r. Komisja Europejska poinformowała władze Stanów Zjednoczonych, że przepisy te mogą być jednak sprzeczne z prawodawstwem unijnym dotyczącym ochrony danych osobowych. Podjęte zostały negocjacje, w wyniku których Departament Bezpieczeństwa Wewnętrznego oraz Biuro Celne i Ochrony Granic USA przyjęły na siebie określone zobowiązania w zakresie ochrony danych. Dnia 14 maja 2004 r. Komisja wydała decyzję 2004/535/WE w sprawie odpowiedniej ochrony zawartych w PNR danych osobowych pasażerów lotniczych, przekazywanych do Biura Celnego i Ochrony Granic Stanów Zjednoczonych[7]. Następnie w dniu 17 maja 2004 r. Rada wydała decyzję 2004/496/WE w sprawie zawarcia porozumienia pomiędzy Wspólnotą Europejską a Stanami Zjednoczonymi Ameryki w sprawie przetwarzania i przekazywania danych dotyczących PNR przez przewoźników lotniczych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych oraz Biura Celnego i Ochrony Granic[8]. Jednakże obie decyzje zostały uznane przez Trybunał Sprawiedliwości UE za nieważne. W ocenie Trybunału decyzja dotycząca odpowiedniej ochrony nie wchodziła w zakres regulacji dyrektywy 95/46/WE, jako że przekazywanie danych następuje w ramach ustanowionych przez władze publiczne i mających na celu ochronę bezpieczeństwa publicznego, a więc zachodzi wyłączenie z art. 3 ust. 2 tiret pierwsze dyrektywy 95/46/WE[9]. Natomiast w odniesieniu do decyzji dotyczącej zawartego porozumienia Trybunał uznał, że została ona wydana według niewłaściwej podstawy prawnej[10]. Trybunał Sprawiedliwości utrzymał jednak w mocy skutki decyzji o odpowiedniej

stantinou, *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, "New Journal of European Criminal Law", No. 2/2015, s. 161.

[7] 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, s. 11.

[8] 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, s. 83. Porozumienie to zostało podpisane 28 maja 2014 r. i weszło w życie tego samego dnia.

[9] Wyrok Trybunału Sprawiedliwości z dnia 30 maja 2006 r., sprawy połączone: C-317/04 i 318/04, pkt 58.

[10] Ibidem.

ochronie do dnia 30 września 2006 r., dając tym samym czas na uregulowanie tych kwestii w sposób zgodny z prawem. W 2007 r. zostało podpisane nowe porozumienie między Unią Europejską a Stanami Zjednoczonymi, dotyczące przetwarzania i transferu danych w ramach PNR[11]. W 2012 r. umowa ta została zastąpiona kolejną, trzecią już umową między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych[12]. Umowa ta reguluje, że DHS przetwarza i wykorzystuje dane PNR w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości międzynarodowej oraz ich wykrywania, prowadzenia dochodzeń lub śledztw oraz ścigania[13]. Wymaga w tym miejscu podkreślenia, że uzgodnienia dotyczące przekazywania danych PNR w celu zwalczania terroryzmu i przestępczości zorganizowanej zostały również podpisane między UE a Kanadą[14] i Australią[15].

[11] Umowa między Unią Europejską a Stanami Zjednoczonymi Ameryki o przetwarzaniu i przekazywaniu przez przewoźników lotniczych danych dotyczących przelotu pasażera (PNR) do Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych (DHS) (Umowa PNR z 2007 r.), Dz. Urz. UE L 204 z 04.08.2007, s. 18.

[12] Dz. Urz. UE L 215 z dnia 11.08.2012 r., s. 5. Zgodnie z art. 26 tej umowy: „Z zastrzeżeniem art. 25 niniejsza umowa pozostaje w mocy przez okres siedmiu lat od dnia jej wejścia w życie" – do 1.07.2019 r.

[13] Zob. tekst preambuły Umowy między Stanami Zjednoczonymi Ameryki a Unią Europejską o wykorzystywaniu danych dotyczących przelotu pasażera oraz przekazywaniu takich danych do Departamentu Bezpieczeństwa Wewnętrznego USA.

[14] Wniosek dotyczący decyzji Rady w sprawie zawarcia umowy między Kanadą a Unią Europejską o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera, COM(2013) 528 wersja ostateczna. Umowa ta została podpisana w 2014 r. Aczkolwiek umowa ta nie weszła jeszcze w życie, ponieważ Parlament Europejski wystąpił do Trybunału Sprawiedliwości o zbadanie, czy proponowana umowa jest zgodna z prawem unijnym, które gwarantuje poszanowanie życia prywatnego i rodzinnego oraz ochronę danych osobowych. Zob. Rezolucja Parlamentu Europejskiego z dnia 25 listopada 2014 r. w sprawie zasięgnięcia opinii Trybunału Sprawiedliwości na temat zgodności z traktatami Umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych dotyczących przelotu pasażera (PNR) (2014/2966(RSP)). W wydanej opinii Rzecznik Generalny P. Mengozzi stwierdził, że niektóre postanowienia umowy są w ich obecnym brzmieniu sprzeczne z Kartą praw podstawowych UE. Szerzej zob. Opinia 1/15 Rzecznika Generalnego P. Mengozziego z dnia 8 września 2016 r. oraz Opinia 1/15 TSUE z dnia 26 lipca 2017 r., w której Trybunał stwierdził, że umowa o przekazywaniu i przetwarzaniu danych dotyczących przelotu pasażera przewidziana między Unią Europejską a Kanadą nie może zostać zawarta w obecnej postaci z powodu niezgodności wielu jej postanowień z prawami podstawowymi uznanymi przez Unię.

[15] 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.

Na konieczność uregulowania przedmiotowej materii na szczeblu unijnym Rada Europejska zwróciła uwagę w „Programie sztokholmskim – otwarta i bezpieczna Europa dla dobra i ochrony obywateli" z 2010 r., apelując do Komisji Europejskiej o przygotowanie przepisów zapewniających wysoki poziom ochrony danych dotyczących przelotu pasażera (PNR) w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia dochodzeń w ich sprawie i ich ścigania[16].

Wniosek dotyczący dyrektywy Parlamentu Europejskiego i Rady w sprawie wykorzystania danych PNR został przedłożony w 2011 r.[17] Zgodnie z jego założeniami linie lotnicze byłyby zobowiązane przekazywać władzom dane osób wjeżdżających na terytorium Unii Europejskiej lub je opuszczających, a państwa członkowskie musiałyby stworzyć krajowe systemy danych pasażerów oparte na wspólnych unijnych zasadach. Biorąc pod uwagę opinię Europejskiego Komitetu Ekonomiczno-Społecznego[18], opinię Europejskiego Inspektora Ochrony Danych[19] i opinię Agencji Praw Podstawowych Unii Europejskiej[20], Parlament Europejski odrzucił jednak projekt dyrektywy w 2013 r.[21] Jako główny zarzut wskazano m.in., że nie uzasadniono w wystarczający sposób potrzeby powszechnego i nieograniczonego korzystania z danych PNR wszystkich pasażerów lotów międzynarodowych, co nie odpowiadało wymogom konieczności i proporcjonalności ingerencji w prawo do prywatności i ochrony danych osobowych wyrażonych w Karcie praw podstawowych UE[22].

Ponownie wrócono do tematu dyrektywy dotyczącej danych PNR po zamachu terrorystycznym na redakcję francuskiego magazynu satyrycz-

[16] Rada Europejska, „Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli" (2010/C 115/01), Dz. Urz. UE C 115 z 4.5.2010, s. 19.

[17] Wniosek dotyczący 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) 32 wersja ostateczna.

[18] Opinia Europejskiego Komitetu Ekonomiczno-Społecznego z dnia 5 maja 2011 r., Dz. Urz. UE C 218 z 23.7.2011, s. 107.

[19] Opinia Europejskiego Inspektora Ochrony Danych z dnia 25 marca 2011 r., Dz. Urz. UE C 181 z 22.6.2011, s. 24.

[20] Opinia Agencji Praw Podstawowych Unii Europejskiej z dnia 14 czerwca 2011 r., FRA Opinion – 1/2011.

[21] 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.

[22] Ibidem.

nego Charlie Hebdo w Paryżu 7 stycznia 2015 r.[23] W dniu 20 listopada 2015 r., zaraz po kolejnym zamachu terrorystycznym w Paryżu, zebrała się Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych, która zwróciła uwagę na konieczną i pilną potrzebę uchwalenia dyrektywy o danych PNR do końca 2015 r.[24] Jeszcze w grudniu tego samego roku Parlament i Rada wypracowały kompromis w sprawie dyrektywy o rejestrze danych pasażerów (PNR), o której będzie mowa dalej. 27 kwietnia 2016 r. 28 krajów członkowskich Unii Europejskiej przyjęło dyrektywę Parlamentu Europejskiego i Rady UE nr 2016/681.

Zakres przedmiotowy dyrektywy 2016/681

Dyrektywa 2016/681 reguluje przekazywanie przez przewoźników lotniczych danych dotyczących przelotu pasażera (danych PNR), które dotyczą pasażerów lotów pozaunijnych, oraz przetwarzanie danych PNR, w tym ich zbieranie, wykorzystywanie i zatrzymywanie przez państwa członkowskie oraz wymianę tych danych między państwami członkowskimi[25].

Dane PNR są przekazywane wyłącznie w tzw. trybie „push". Jest to „metoda dostarczania", która polega na tym, że przewoźnicy lotniczy przekazują (ang. *push*) potrzebne dane PNR danemu organowi na jego wniosek, co pozwala im zachować kontrolę nad tym, jakie dane są przekazywane[26]. Przyjmuje się, że „metoda dostarczania" zapewnia wyższy poziom ochrony danych[27].

Zgodnie z art. 3 pkt 2 dyrektywy „lot pozaunijny" oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z państwa trzeciego z zaplanowanym lądowaniem na terytorium państwa członkowskiego albo odbywający się z terytorium państwa członkowskiego z zaplanowanym lądowaniem w państwie trzecim, w tym – w obu przypadkach – loty z postojami na terytorium państw członkowskich lub państw trzecich. Należy jednak zauważyć, iż w art. 2 dyrektywy przyznano państwom członkowskim pewien margines uznania co do

[23] N. Vavoula, *'I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive*, 26.10.2016 r., http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/ (dostęp 6.06.2017).

[24] Informacja dostępna na stronie: http://www.consilium.europa.eu/pl/meetings/jha/2015/11/20/ (dostęp 10.06.2017).

[25] Art. 1 dyrektywy. Zob. także art. 11 dyrektywy.

[26] Motyw 16 dyrektywy.

[27] Zob. C. Blasi Casagran, op.cit.; A. Rizer, *Dog Fight: Did The International Battle Over Airline Passenger Name Records Enable The Christmas-day Bomber?*, "Catholic University Law Review", No. 1/2010, s. 77–105.

możliwości stosowania niniejszej dyrektywy także do lotów wewnątrzunijnych, zastrzegając jednocześnie, że chodzi jedynie o wybrane loty wewnątrzunijne[28]. Państwo członkowskie dokonuje wyboru lotów wewnątrzunijnych, które uważa za niezbędne z punktu widzenia realizacji celów niniejszej dyrektywy. Jednakże o tym fakcie państwo członkowskie jest obowiązane powiadomić Komisję Europejską w formie pisemnej[29].

W dyrektywie *expressis verbis* wskazano, że dane PNR mogą być przetwarzane jedynie w celach zapobiegania przestępstwom terrorystycznym i poważnej przestępczości oraz ich wykrywania, prowadzenia postepowań przygotowawczych w ich sprawie i ich ścigania. Dodano, że definicja przestępstw terrorystycznych przyjęta na potrzeby przedmiotowej dyrektywy powinna być taka sama, jak definicja w decyzji ramowej Rady 2002/475/WSiSW[30]. Zgodnie z tą regulacją za „przestępstwa terrorystyczne" są uważane następujące czyny: ataki na życie ludzkie, które mogą powodować śmierć; ataki na integralność cielesną osoby; porwania lub branie zakładników; spowodowanie rozległych zniszczeń obiektów rządowych lub obiektów użyteczności publicznej, systemu transportowego, infrastruktury, włącznie ze zniszczeniem systemu informacyjnego, stałych platform umieszczonych na szelfie kontynentalnym, miejsca publicznego lub mienia prywatnego, mogące zagrozić życiu ludzkiemu lub mogące spowodować poważne straty gospodarcze; zajęcie statku powietrznego, statku lub innego środka transportu publicznego lub towarowego; wytwarzanie, posiadanie, nabywanie, przewożenie, dostarczanie lub używanie broni, materiałów wybuchowych lub jądrowych, broni biologicznej lub chemicznej, jak również badania i rozwój broni biologicznej i chemicznej; uwalnianie substancji niebezpiecznych lub powodowanie pożarów, powodzi lub wybuchów, których rezultatem jest zagrożenie życia ludzkiego; zakłócenia lub przerwy w dostawach wody, energii elektrycznej lub wszelkich innych podstawowych zasobów naturalnych, których rezultatem jest zagrożenie życia ludzkiego; oraz grożenie popełnieniem ww. czynów[31]. Natomiast pod pojęciem poważnej przestępczości należy rozumieć przestępstwa wymienione w załączniku II do niniejszej dyrektywy, które na mocy prawa krajowego państwa członkowskiego podlegają karze pozbawienia wolno-

[28] Zgodnie z art. 3 pkt 3 lot „wewnątrzunijny" oznacza regularny lub nieregularny lot, obsługiwany przez przewoźnika lotniczego, odbywający się z terytorium państwa członkowskiego, z zaplanowanym lądowaniem na terytorium co najmniej jednego innego państwa członkowskiego, bez postojów na terytorium państwa trzeciego.

[29] Art. 2 ust. 1 dyrektywy.

[30] Decyzja ramowa Rady 2002/475/WSiSW z dnia 13 czerwca 2002 r. w sprawie zwalczania terroryzmu, Dz. Urz. UE L 164 z 22.6.2002, s. 3.

[31] Art. 1 ust. 1 Decyzji ramowej Rady 2002/475/WSiSW.

ści lub środkowi zabezpieczającemu polegającemu na pozbawieniu wolności o maksymalnym wymiarze co najmniej trzech lat. Katalog tych przestępstw ma charakter zamknięty i obejmuje 26 czynów karalnych.

Omawiana dyrektywa stanowi, że dane PNR powinny zawierać wyłącznie informacje dotyczące rezerwacji i tras podróży pasażerów, które mają umożliwić właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego[32]. Jak wynika z motywu 15 dyrektywy, z wykazu danych PNR zostały wyłączone dane wrażliwe, takie jak: rasa, pochodzenie etniczne, religia, poglądy polityczne i jakiekolwiek inne poglądy, przynależność do związków zawodowych, stan zdrowia, życie seksualne, orientacja seksualna danej osoby. Co więcej, w celu wyeliminowania potencjalnych nadużyć w załączniku I sprecyzowano, jakie dokładnie dane będą gromadzone. Analizując te dane, które obejmują 19 kategorii, nasuwa się jednak wątpliwość, czy zostały one sformułowane w sposób jasny i precyzyjny, w szczególności pkt 12 zatytułowany „uwagi ogólne (w tym wszelkie dostępne informacje o osobach małoletnich bez opieki w wieku poniżej 18 lat, takie jak: imię i nazwisko, płeć, wiek, języki, którymi włada, imię i nazwisko oraz dane kontaktowe opiekuna w momencie odlotu i rodzaj więzi łączącej go z osobą małoletnią, imię i nazwisko oraz dane kontaktowe opiekuna w momencie lądowania i rodzaj więzi łączącej go z osobą małoletnią, przedstawiciel obecny przy odlocie i przylocie)". Należy zauważyć, że obejmują one również informacje dotyczące preferencji żywieniowych pasażerów podczas lotu, które mogą dostarczać wskazówek na temat ich pochodzenia etnicznego czy przekonań religijnych. Oznacza to, że w ramach przetwarzania danych PNR może *de facto* dochodzić do ujawniania danych wrażliwych na podstawie pkt 12 załącznika I. Wprawdzie dyrektywa ustanawia pewne zabezpieczenia, aby zagwarantować, że przekazane dane nie wykroczą poza wykaz elementów podany w załączniku I. Z art. 6 ust. 1 i art. 13 ust. 4 wynika bowiem, że jeżeli wśród danych PNR przekazanych przez przewoźników lotniczych znajdują się dane inne niż wymienione w załączniku I, a także dane wrażliwe, jednostka do spraw informacji o pasażerach usuwa takie dane w sposób trwały niezwłocznie po ich otrzymaniu. Mając jednak na względzie ryzyko stygmatyzacji niektórych pasażerów, niebędących podejrzanymi o jakiekolwiek przestępstwo, należałoby postulować doprecyzowanie ww. kategorii danych w celu wyraźnego zapewnienia, że dane o pochodzeniu etnicznym pasażera czy jego wyznaniu nie będą ujawniane na podstawie niniejszej dyrektywy.

[32] Motyw 15 dyrektywy.

Przetwarzanie danych PNR jako środek adekwatny do celu?

Gdy analizuje się przepisy dyrektywy 2016/681, należy zauważyć, że prawodawca europejski ma świadomość ingerencji związanej z przekazywaniem, wykorzystywaniem, zatrzymywaniem danych PNR, ponieważ – jak wyraźnie wynika z jej preambuły – właśnie ze względu na tę ingerencję niniejsza dyrektywa podejmuje próbę pogodzenia wymagań dotyczących bezpieczeństwa publicznego oraz poszanowania praw podstawowych do ochrony prywatności i danych osobowych[33]. W dyrektywie wskazano, że przetwarzanie danych osobowych pasażerów powinno być proporcjonalne do szczególnych celów dotyczących bezpieczeństwa, którym służy niniejsza regulacja. W dyrektywie uwzględniono także najnowsze orzecznictwo Trybunału Sprawiedliwości Unii Europejskiej w zakresie ochrony danych osobowych, zapewniając, że przy jej stosowaniu będą respektowane prawa podstawowe[34]. Warto zatem odwołać się do dwóch wyroków TSUE w sprawach *Digital Rights*[35] i *Schrems*[36], w których Trybunał ustanowił aktualne wymogi ochrony danych osobowych w prawie unijnym. W wyroku z dnia 8 kwietnia 2014 r. Trybunał podniósł dwie bardzo istotne kwestie. Po pierwsze, Trybunał podkreślił, że regulacje unijne muszą zawierać jasne i dokładne postanowienia dotyczące zakresu i sposobu środków ingerujących w dane osobowe[37]. Po drugie, regulacje te muszą zawierać minimalne zabezpieczenia służące temu, aby osoby, których dane zostały zatrzymane, miały wystarczające gwarancje rzeczywistej ochrony ich danych osobowych przed ryzykiem nadużyć oraz ich bezprawnym udostępnianiem i wykorzystywaniem[38]. Trybunał stwierdził, że zatrzymywanie danych osobowych w celu ich ewentualnego udostępnienia właściwym organom krajowym pozostaje w bezpośrednim i szczególnym związku z prawem do poszanowania ży-

[33] Zob. Motyw 20 i 22 dyrektywy.

[34] Motyw 22 dyrektywy.

[35] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone: C-293/12 i C-594/12.

[36] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., sprawa C-362/14.

[37] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone: C-293/12 i C-594/12, pkt 54. Szerzej zob. M. Granger, K. Irion, *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, "European Law Review", No. 6/2014, s. 835–854.

[38] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone: C-293/12 i C-594/12, pkt 54.

cia prywatnego, a tym samym – z prawami, które zostały zagwarantowane w art. 7 KPP[39]. Takie zatrzymywanie danych jest objęte również zakresem zastosowania art. 8 Karty, gdyż stanowi przetwarzanie danych osobowych w rozumieniu tego artykułu i jako takie musi spełniać wynikające z niego wymogi w zakresie ochrony danych. W świetle art. 8 KPP dane osobowe muszą być przetwarzane rzetelnie w określonych celach i za zgodą osoby zainteresowanej lub na innej uzasadnionej podstawie przewidzianej ustawą; każdy ma prawo dostępu do zebranych danych, które go dotyczą, i prawo do dokonania ich sprostowania; przestrzeganie tych zasad podlega kontroli niezależnego organu. Ponadto Trybunał po raz kolejny przypomniał, że zasada proporcjonalności wymaga, by akty prawne instytucji Unii były odpowiednie do realizacji uzasadnionych celów, którym akty te służą, i nie wykraczały poza to, co jest konieczne do ich osiągnięcia[40]. Ochrona prawa do poszanowania życia prywatnego „w każdym wypadku wymaga, aby odstępstwa od ochrony danych osobowych i jej ograniczenia ograniczały się do tego, co absolutnie konieczne"[41]. Trybunał wskazał, że zbieranie danych osobowych musi być ograniczone do danych związanych albo z określonym czasem, określonym obszarem geograficznym lub określonym kręgiem osób mogących, w taki czy inny sposób, mieć związek z poważnym przestępstwem, albo osobami, których zatrzymane dane z innych powodów mogłyby przyczynić się do zapobiegania poważnym przestępstwom oraz ich wykrywania lub ścigania[42]. Co więcej, Trybunał wyraził pogląd, że wrażenia i odczucia wzbudzone u osób, do których odnoszą się przepisy dotyczące przetwarzania i zatrzymywania danych osobowych, mają duże znaczenie w kontekście oceny wagi ingerencji w prawa podstawowe gwarantowane w art. 7 i art. 8 ust. 1 KPP[43].

Z kolei w wyroku z dnia 6 października 2015 r. TSUE uznał m.in., że „uregulowanie nieprzewidujące dla jednostek żadnej drogi prawnej w celu uzyskania dostępu do dotyczących ich danych osobowych lub sprostowania czy usunięcia takich danych nie zapewnia poszanowania zasadniczej istoty prawa podstawowego do skutecznej ochrony prawnej, wynikającego z art. 47 karty [...]"[44].

[39] „Każdy ma prawo do poszanowania życia prywatnego i rodzinnego, domu i komunikowania się".

[40] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone: C-293/12 i C-594/12, pkt 46.

[41] Ibidem, pkt 52.

[42] Ibidem, pkt 59.

[43] Ibidem, pkt 37.

[44] Wyrok Trybunału Sprawiedliwości z dnia 6 października 2015 r., sprawa C-362/14, pkt 95.

Wymóg przydatności przetwarzania danych PNR

Podczas analizy przepisów dyrektywy 2016/681 z punktu widzenia zasady proporcjonalności należy zbadać w pierwszej kolejności, czy przewidziana w dyrektywie ingerencja w postaci przetwarzania danych PNR jest w stanie doprowadzić do osiągnięcia celu związanego z bezpieczeństwem publicznym. Zgodnie z art. 52 ust. 1 KPP prawa podstawowe, takie jak prawo do poszanowania życia prywatnego i ochrony danych osobowych, nie mają charakteru bezwzględnego, lecz mogą podlegać ograniczeniom, pod warunkiem że ograniczenia te rzeczywiście odpowiadają celom interesu ogólnego, jakim służy dany środek, i że nie stanowią, z punktu widzenia realizowanych celów, nieproporcjonalnej oraz niedopuszczalnej ingerencji zagrażającej samej istocie praw w ten sposób gwarantowanych. Podstawowym celem przedmiotowej dyrektywy „jest zapewnienie bezpieczeństwa ogólnego, ochrona życia i bezpieczeństwa osób oraz stworzenie ram prawnych służących ochronie danych PNR w związku z ich przetwarzaniem przez właściwe organy”[45]. Cel ten ma być osiągnięty za pomocą sprawdzania danych PNR umożliwiającego identyfikację osób uprzednio „nieznanych”, tzn. osób, które przed dokonaniem takiego sprawdzenia nie były wcześniej podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości, lecz w odniesieniu do których analiza danych sugeruje, że mogą być zamieszane w taką działalność przestępczą[46]. Jak podkreśla się w literaturze, dane PNR mają bowiem ważne zastosowanie w identyfikacji potencjalnych terrorystów[47]. Należy zauważyć, że nawet dane sprzed kilku lat w postaci *inter alia*: adresów, numerów telefonicznych, adresów poczty elektronicznej, a także numerów, jakie osoby często podróżujące posiadają w ramach programu lojalnościowego *frequent flyer*, mogą mieć zasadnicze znaczenie dla znalezienia powiązań między osobami podejrzanymi o prowadzenie działalności terrorystycznej czy przestępczości zorganizowanej (np. handel ludźmi, narkotykami)[48]. Ponadto doświadczenia innych państw, m.in. Stanów Zjednoczonych i Wielkiej Brytanii, pokazują, że wykorzystywanie danych PNR pozwoliło uzyskać

[45] Motyw 5 dyrektywy.

[46] Wniosek dotyczący 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) 32 wersja ostateczna, s. 5.

[47] Zob. szerzej: D. Lowe, op.cit., s. 101; A. Rizer, op.cit., s. 100–101; M.R. Van-Wasshnova, *Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System Of Financial Information Exchange*, “Case Western Reserve Journal of International Law”, No. 3/2007, s. 864.

[48] Ibidem.

zasadnicze postępy w walce z przestępczością, w szczególności z handlem ludźmi i narkotykami oraz terroryzmem, a także lepiej zrozumieć skład i funkcjonowanie sieci terrorystycznych i innych grup przestępczych[49].

Dodatkowo w dyrektywie zwrócono uwagę, że dzięki wykorzystywaniu danych PNR można reagować na zagrożenie przestępstwami terrorystycznymi i poważną przestępczością z innej perspektywy niż w przypadku przetwarzania pozostałych kategorii danych osobowych[50]. Rzeczywistym celem tej dyrektywy jest więc przyczynianie się do walki z działalnością terrorystyczną i poważną przestępczością, co w ostatecznym rozrachunku przekłada się na zapewnienie bezpieczeństwa publicznego. W orzecznictwie TSUE przyjęto bowiem, że walka z terroryzmem w celu utrzymania międzynarodowego pokoju i bezpieczeństwa stanowi cel interesu ogólnego UE[51]. Analogicznie rzecz ma się w przypadku walki z poważną przestępczością, prowadzoną w celu zapewnienia bezpieczeństwa publicznego[52]. Co więcej, warto zauważyć, że zarówno rzecznik generalny P. Mengozzi, jak i Trybunał Sprawiedliwości w Opinii na temat zgodności z traktatami Umowy między Kanadą a Unią Europejską w sprawie przekazywania i przetwarzania danych dotyczących przelotu pasażera (PNR) stwierdzili, że przekazywanie danych PNR jest „przydatne do zapewnienia osiągnięcia celu przewidywanej umowy związanego z zapewnieniem ochrony publicznej i bezpieczeństwa publicznego"[53]. W konkluzji należy uznać, że ustanowiony w dyrektywie 2016/681 obowiązek przetwarzania danych PNR realizuje cel interesu ogólnego w rozumieniu art. 52 ust. 1 KPP.

Wymóg niezbędności i proporcjonalności *sensu stricto* przetwarzania danych PNR

Następnie należy ocenić, czy przewidziana w dyrektywie ingerencja jest niezbędna dla ochrony interesu ogólnego oraz czy efekty wprowadzonej ingerencji pozostają w odpowiedniej proporcji do ciężarów nakładanych przez nią na jednostkę. Wykorzystywanie danych PNR, m.in. przez porównanie danych PNR z danymi zawartymi w różnych bazach

[49] Zob. A. Rizer, op.cit., s. 94. Dzięki danym PNR w grudniu 2009 r. udaremniono próbę ataku terrorystycznego na pokładzie samolotu z Amsterdamu do Detroit.

[50] Motyw 7 dyrektywy.

[51] Wyrok Trybunału Sprawiedliwości z dnia 3 września 2008 r., sprawy połączone: C-402/05 P i C-415/05 P, pkt 363. Zob. także: Wyrok Trybunału Sprawiedliwości z dnia z dnia 15 listopada 2012 r., sprawy połączone: C-539/10 P i C-550/10 P, pkt 130.

[52] Wyrok Trybunału Sprawiedliwości z dnia 23 listopada 2010 r., sprawa C-145/09, pkt 46, 47.

[53] Zob. Opinia 1/15 Rzecznika Generalnego P. Mengozziego z dnia 8 września 2016 r. oraz Opinia 1/15 TSUE z dnia 26 lipca 2017 r.

danych poszukiwanych osób i przedmiotów, umożliwia zebranie dowodów, a – w odpowiednich przypadkach – wykrycie sprawców określonych przestępstw i rozpracowanie grup przestępczych[54]. W doktrynie pojawiają się jednak argumenty, że przedmiotowa dyrektywa pozwala przetwarzać i analizować dane milionów pasażerów lotów międzynarodowych, którzy nigdy nie popełnili żadnego z przestępstw wymienionych w dyrektywie, wskazując, że w identyfikowaniu niebezpiecznych przestępców będą wykorzystywane określone dane osób niewinnych[55]. Jak zauważają P. De Hert i V. Papakonstantinou, dane PNR są przetwarzane nawet wtedy, gdy nie ma wobec nich żadnych podstaw, nawet pośrednich, do wszczęcia postępowania karnego[56]. Autorzy podnoszą, że przedmiotowa dyrektywa ma zastosowanie wobec osób, co do których brak jest dowodów mogących sugerować, że ich zachowanie może mieć jakikolwiek związek z terroryzmem lub poważnymi przestępstwami, co w konsekwencji budzi wątpliwości z punktu widzenia zasady domniemania niewinności[57]. Ich zdaniem, może to u obywateli wywoływać poczucie, że ich życie prywatne podlega masowej inwigilacji[58]. Odnosząc się do powyższych argumentów, należy zgodzić się co do kwestii, iż wspomniane dane PNR wymienione w załączniku I do niniejszej dyrektywy, są przekazywane właściwemu organowi w odniesieniu do wszystkich pasażerów korzystających z lotów pozaunijnych, bez żadnych przesłanek świadczących o tym, że ich zachowanie może mieć związek z działalnością terrorystyczną lub poważną przestępczością. Jednakże, jak wyjaśniono w uzasadnieniu do projektu dyrektywy, istotą systemów PNR jest właśnie zapewnienie masowego przekazywania danych pozwalających właściwym organom na zidentyfikowanie, za pomocą systemów zautomatyzowanego przetwarzania danych lub określonych wcześniej kryteriów oceny, osób nieznanych organom ścigania, które mogą stanowić zagrożenie dla bezpieczeństwa publicznego i które w związku z tym mogą zostać następnie poddane dalszym kontrolom. Wymaga bowiem podkreślenia, że cel prewencyjny nie mógłby zostać osiągnięty, gdyby przekazywano tylko dane PNR poszukiwanych osób podejrzanych.

Na podstawie przepisów dyrektywy właściwe organy muszą wykorzystywać dane PNR na bieżąco w celu porównania ich z określonymi wcześniej kryteriami oceny, co wskazuje, które „nieznane" wcześniej osoby

[54] Zob. motyw 6 dyrektywy.
[55] P. De Hert, E. Papakonstantinou, op.cit., s. 163–164; N. Vavoula, op.cit.
[56] P. De Hert, E. Papakonstantinou, op.cit., s. 163.
[57] Ibidem.
[58] Ibidem.

wymagają dalszej kontroli[59]. Dzięki sprawdzeniu danych PNR w czasie rzeczywistym na podstawie odpowiednich kryteriów można zapobiec przestępstwom lub je wykryć. Przykładowo, analiza danych PNR może wskazać, jakie są najczęściej wybierane szlaki przerzutu osób lub narkotyków, co może stanowić element kryteriów oceny. Należy podkreślić, że w wyniku czterech zamachów terrorystycznych, które miały miejsce w przeciągu ostatnich dwóch lat w Europie, tj. w styczniu i listopadzie 2015 r. w Paryżu, w marcu 2016 r. w Brukseli i w maju 2017 r. w Manchesterze, zginęło przeszło 200 osób, w tym również dzieci. Warto zwrócić uwagę, że sprawcy tych zamachów przed ich dokonaniem podróżowali zarówno do różnych krajów unijnych, jak i do państw spoza UE. Szacuje się, że ok. 5 tys. obywateli Unii Europejskiej dołączyło do organizacji terrorystycznych w Iraku i Syrii, w związku z czym osoby te mogą stanowić zagrożenie dla bezpieczeństwa w Unii[60]. Co więcej, jak wynika z raportu Europolu, większość działań terrorystycznych ma charakter transgraniczny i wiąże się z podróżami międzynarodowymi do obozów szkoleniowych zlokalizowanych poza UE[61]. Wobec powyższego należy zatem uznać, że ingerencja, jaką przewiduje przedmiotowa dyrektywa, jest odpowiednia i niezbędna do osiągnięcia realizowanego przez nią celu związanego z bezpieczeństwem publicznym, w szczególności z zapobieganiem przestępstwom terrorystycznym i poważnej przestępczości.

W celu zapewnienia przejrzystości dane PNR są przekazywane przez przewoźników lotniczych jednostce do spraw informacji o pasażerach (zwanej dalej „JIP"). JIP jest to organ, który każde państwo członkowskie jest zobowiązane ustanowić. Do zadań JIP należy zbieranie od przewoźników lotniczych danych PNR, ich przechowywanie i przetwarzanie oraz wymiana zarówno danych PNR, jak i wyników ich przetwarzania z JIP w innych państwach członkowskich i z Europolem[62]. W art. 6 dyrektywy wskazano trzy konkretne cele przetwarzania danych PNR przez JIP. Obejmują one:

1) dokonanie sprawdzenia pasażerów przed ich planowanym przylotem do lub odlotem z państwa członkowskiego w celu identyfikacji

[59] Zob. Wniosek dotyczący 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) 32 wersja ostateczna, s. 6.

[60] Informacja pochodzi ze strony internetowej: http://www.europarl.europa.eu/news/pl/headlines/security/20160404STO21310/poslowie-beda-dyskutowac-o-unijnej-strategii-walki-z-terroryzmem (dostęp 10.06.2017).

[61] Sprawozdanie Europolu dotyczące sytuacji i tendencji w dziedzinie terroryzmu w UE z roku 2010.

[62] Art. 4 ust. 2 dyrektywy.

osób, które wymagają dalszego sprawdzenia przez właściwe organy oraz – w stosownych przypadkach – przez Europol, ze względu na możliwość udziału takich osób w przestępstwach terrorystycznych lub w poważnej przestępczości;
2) odpowiadanie, na podstawie oceny każdego indywidualnego przypadku, na należycie uzasadniony i oparty na wystarczających podstawach wniosek właściwych organów o przekazanie i przetwarzanie danych PNR w określonych przypadkach w celach zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, oraz o przekazanie właściwym organom lub – w stosownych przypadkach – Europolowi[63] wyników takiego przetwarzania;
3) analizowanie danych PNR do celów aktualizacji lub tworzenia nowych kryteriów stosowanych przy sprawdzeniach z zamiarem identyfikacji wszystkich osób, które mogą brać udział w przestępstwach terrorystycznych lub w poważnej przestępczości[64].

Dokonując sprawdzenia, JIP może porównywać dane PNR z bazami danych, które mają znaczenie dla zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, w tym z bazami danych o osobach lub przedmiotach poszukiwanych lub objętych wpisem, zgodnie z przepisami unijnymi, międzynarodowymi i krajowymi mającymi zastosowanie do takich baz danych[65]. JIP może również przetwarzać dane PNR według wcześniej ustalonych kryteriów. Należy jednak zauważyć, że w dyrektywie nie zawarto szczegółowych przepisów, które odnosiłyby się do zasad i metod tworzenia tych baz danych. Nie wyjaśniono również, o jakie konkretne kryteria oceny chodzi. Ich określenie pozostawiono w gestii państw członkowskich, co w konsekwencji może budzić poważne wątpliwości, czy dyrektywa rzeczywiście ustanawia ramy prawne przewidujące jednolite gwarancje i zabezpieczenia ochrony danych PNR dla wszystkich obywateli UE. Wprawdzie w dyrektywie wskazano, że „wcześniej ustalone kryteria muszą być ukierunkowane, proporcjonalne i szczegółowe" i sprawdzanie danych PNR na ich podstawie odbywa się w sposób niedyskryminacyjny[66]. Państwa członkowskie są zobowiązane zapewnić, aby kryteria te były ustanawiane i poddawane regularnym prze-

[63] Zob. art. 10 dyrektywy.
[64] Art. 6 ust. 2 dyrektywy.
[65] Art. 6 ust. 3 dyrektywy.
[66] Art. 6 ust. 4 dyrektywy.

glądom przez JIP we współpracy z właściwymi organami[67]. Dodano, że „kryteria dokonywania sprawdzeń powinny zostać określone w taki sposób, by ograniczyć do minimum liczbę osób niewinnych błędnie zidentyfikowanych przez system"[68]. W art. 6 ust. 4 zagwarantowano także, że kryteria te „w żadnym przypadku nie mogą opierać się na rasie ani pochodzeniu etnicznym, na poglądach politycznych, przekonaniach religijnych lub światopoglądowych, przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby". Niemniej jednak należałoby objąć tym przepisem także wykorzystywane bazy danych, z którymi porównywane są dane PNR, tak aby wyraźnie wykluczyć, że wskazane cechy nie mogą być podstawą ich tworzenia. Określenie baz danych i kryteriów oceny powinno – zgodnie z orzecznictwem Europejskiego Trybunału Praw Człowieka – przede wszystkim umożliwić uzyskanie wyników ukierunkowanych na osoby, na których mogłoby ciążyć „uzasadnione podejrzenie" udziału w przestępstwach terrorystycznych lub poważnych przestępstwach[69]. Ponadto w celu spełnienia wymogu konieczności te odpowiednie kryteria i bazy danych, jak również ich analiza powinny podlegać kontroli ze strony niezależnego organu nadzorczego określonego w art. 15 dyrektywy.

Mając na uwadze prawo do ochrony danych osobowych, przetwarzanie danych PNR w każdym państwie członkowskim przez JIP oraz przez właściwe organy podlega standardom ochrony danych osobowych wynikającym z prawa krajowego, zgodnym z decyzją ramową Rady 2008/977/WSiSW[70]. W dyrektywie wyraźnie uregulowano, że państwa członkowskie są zobowiązane zapewnić, aby każdy pozytywny wynik automatycznego przetwarzania danych PNR dokonanego na podstawie sprawdzenia pasażera był indywidualnie oceniany w sposób niezautomatyzowany w celu ustalenia, czy właściwy organ powinien podjąć działania zgodnie z prawem krajowym[71]. Tym samym rozwiązanie to umożliwia zmniejszenie liczby osób poddawanych dalszym, bardziej starannym kontrolom.

Z punktu widzenia przestrzegania zasady proporcjonalności niezbędne jest także zachowanie wysokiego poziomu ochrony danych osobowych pasażerów przed przypadkowym, niezgodnym z prawem lub nieupraw-

[67] Ibidem.

[68] Motyw 7 dyrektywy.

[69] Wyrok ETPC z dnia 4 grudnia 2015 r., *Zakharov p. Rosji*, Skarga nr 47143/06, pkt 260.

[70] Zob. decyzja ramowa Rady 2008/977/WSiSW z dnia 27 listopada 2008 r. w sprawie ochrony danych osobowych przetwarzanych w ramach współpracy policyjnej i sądowej w sprawach karnych (Dz. Urz. L 350 z 30.12.2008, s. 60).

[71] Art. 6 ust. 5 dyrektywy.

nionym dostępem, przetwarzaniem lub utratą. Wiąże się to z koniecznością m.in. zastosowania odpowiednich procedur i środków technicznych zapewniających dostęp do przedmiotowych informacji osobom przeszkolonym w zakresie ich ochrony, które są upoważnione do ich uzyskania lub przetwarzania ze względu na powierzone zadania i obowiązki służbowe. Na podstawie art. 6 ust. 3 dyrektywy „przechowywanie, przetwarzanie i analiza danych PNR przez JIP odbywa się wyłącznie w bezpiecznym miejscu lub bezpiecznych miejscach na terytorium państw członkowskich". Dyrektywa przewiduje, że JIP w każdym państwie członkowskim jest zobowiązana wdrożyć odpowiednie środki techniczne i organizacyjne oraz procedury techniczne i organizacyjne, by zapewnić wysoki poziom bezpieczeństwa odpowiedni do zagrożenia związanego z przetwarzaniem danych PNR oraz do charakteru tych danych. Jednocześnie JIP powołuje inspektora ochrony danych osobowych, który odpowiada za monitorowanie danych PNR. Ponadto państwa członkowskie zapewniają, by inspektor ochrony danych miał dostęp do wszystkich danych przetwarzanych przez JIP. Jeżeli inspektor ochrony danych uzna, że przetwarzanie jakichkolwiek danych było niezgodne z prawem, może przekazać sprawę do krajowego organu nadzorczego[72], który odpowiada za doradztwo i monitorowanie w zakresie stosowania na jego terytorium przepisów niniejszej dyrektywy. Dyrektywa gwarantuje także każdemu pasażerowi prawo do ochrony jego danych osobowych, prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej[73].

Co więcej, zgodnie z art. 13 ust. 4 i ust. 5 przewidziany jest nie tylko obowiązek prowadzenia dokumentacji w przedmiocie wszystkich systemów i procedur przetwarzania danych PNR przez JIP, ale także obowiązek ewidencji operacji przetwarzania tych danych, takich jak: zbieranie, przeglądanie, ujawnianie i usuwanie. Pozytywnie należy ocenić również doprecyzowanie, że dane PNR oraz wyniki przetwarzania tych danych, otrzymane od JIP, mogą być poddane dalszemu przetwarzaniu przez właściwe organy państw członkowskich[74] wyłącznie do celów określonych w art. 1 ust. 2 dyrektywy[75]. Właściwe organy państw członkowskich nie mogą opierać decyzji mającej negatywne skutki prawne dla osoby lub poważnie wpływającej na jej sytuację wyłącznie na wynikach automatycz-

[72] Art. 6 ust. 7 dyrektywy. W przypadku Polski jest to GIODO.

[73] Art. 13 ust. 1 dyrektywy.

[74] Organy te są organami właściwymi do zapobiegania przestępstwom terrorystycznym lub poważnym przestępstwom, ich wykrywania, prowadzenia postepowań przygotowawczych w ich sprawie i ich ścigania.

[75] Art. 7 ust. 4 dyrektywy.

nego przetwarzania danych PNR[76]. Ponadto zapewniono, że taka decyzja nie może opierać się na rasie lub pochodzeniu etnicznym osób, ich przekonaniach religijnych lub światopoglądowych, poglądach politycznych, przynależności do związków zawodowych czy informacjach o zdrowiu lub życiu seksualnym danej osoby[77].

Natomiast jeśli chodzi o wprowadzenie pięcioletniego okresu zatrzymywania danych PNR, po upływie którego dane te zostaną usunięte w sposób trwały, należy zauważyć, że nie spełnia on wymogu ustanowionego przez TSUE w sprawie *Digital Rights*. Odnosząc się do co najmniej dwuletniego okresu, w jakim dane będą zatrzymywane, Trybunał negatywnie ocenił fakt, że dyrektywa 2006/24 nie wskazuje żadnych różnic między kategoriami danych w zależności od zainteresowanych osób lub ewentualnej użyteczności danych w stosunku do zakładanego celu[78]. Co więcej, TSUE powtórzył ten argument w Opinii z dnia 26 lipca 2017 r., wskazując, że „zatrzymywanie danych PNR po wyjeździe pasażerów lotniczych [powinno być ograniczone do tych pasażerów], w odniesieniu do których istnieją obiektywne przesłanki pozwalające na uznanie, że mogliby oni stanowić zagrożenie w rozumieniu zwalczania terroryzmu i poważnych przestępstw międzynarodowych"[79]. Natomiast w dyrektywie 2016/681 wskazano jedynie, że „dane PNR powinny być zatrzymywane na okres niezbędny i proporcjonalny do celów, jakimi są zapobieganie przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywanie, prowadzenie postepowań przygotowawczych w ich sprawie i ich ściganie. Ze względu na charakter danych i ich wykorzystanie niezbędne jest zatrzymywanie danych PNR przez wystarczająco długi okres, aby możliwe było ich analizowanie i wykorzystywanie w postępowaniach przygotowawczych"[80]. Należy mieć na uwadze, że po upływie okresu sześciu miesięcy od przekazania danych PNR przez przewoźników lotniczych JIP, wszystkie dane PNR zostają poddane depersonalizacji przez maskowanie[81] następujących ich elementów mogących posłużyć do bezpośredniej identyfikacji pasażera, którego dotyczą, tj.: imię i nazwisko, adres i dane kontaktowe, informacje o formie płatności i programach lojalnoś-

[76] Art. 7 ust. 6 dyrektywy.

[77] Ibidem.

[78] Wyrok Trybunału Sprawiedliwości z dnia 8 kwietnia 2014 r., sprawy połączone: C-293/12 i C-594/12, pkt 62–64.

[79] Opinia 1/15 TSUE z dnia 26 lipca 2017 r.

[80] Motyw 25 dyrektywy.

[81] Zgodnie z art. 3 pkt 10 dyrektywy „Depersonalizacja poprzez maskowanie elementów danych" oznacza uczynienie niewidocznymi dla użytkownika takich elementów danych, które mogłyby posłużyć do bezpośredniego zidentyfikowania osoby, której dane dotyczą.

ciowych oraz wszelkie dane API[82]. Niemniej jednak zawarte w dyrektywie wyjaśnienie nie wskazuje obiektywnych powodów, które uzasadniałyby konieczność zatrzymywania wszystkich danych PNR właśnie przez okres pięciu lat. Pożądane byłoby zatem doprecyzowanie tego przepisu przez dodanie dodatkowych kryteriów, jak wskazał TSUE.

Podsumowanie

Ostatnie zamachy terrorystyczne w Europie ukazują, że zagrożenie terroryzmem w Europie jest nadal znaczne i stale ewoluuje. W rezultacie niezbędne jest podejmowanie przez władze publiczne na szczeblu unijnym odpowiednich środków zapobiegawczych m.in. w postaci zacieśnionej współpracy między organami ścigania w odniesieniu do pasażerów lotów międzynarodowych z i do państw członkowskich, w tym bardziej systematycznego wykorzystywania danych dotyczących przelotu takich pasażerów (PNR) na potrzeby ochrony bezpieczeństwa i życia obywateli. Decydując się na uregulowanie tej materii w dyrektywie 2016/681, prawodawca europejski stanął przed koniecznością osiągnięcia właściwej równowagi między zwalczaniem terroryzmu i poważnej przestępczości a ochroną danych osobowych przy jednoczesnym poszanowaniu prywatności osób, których dane dotyczą. Osiągnięcie tej równowagi powinno znaleźć wyraz w jasnych i precyzyjnych przepisach przedmiotowej dyrektywy. Nie ulega wątpliwości, że dane PNR, które mają być przetwarzane na podstawie niniejszej dyrektywy, dają krajowym organom ścigania dodatkowe możliwości w zakresie zapobiegania i wykrywania przestępstw terrorystycznych i innych poważnych przestępstw, i z tego względu stanowią dla nich cenne narzędzie przy prowadzeniu czynności dochodzeniowo-śledczych. Jednakże przetwarzanie danych PNR stanowi zarazem ingerencję w prawa podstawowe jednostek, która – aby była zgodna z prawem – musi spełniać wymogi zasady proporcjonalności. Analiza przepisów omawianej dyrektywy ukazuje, że przewidziana w dyrektywie ingerencja odpowiada celowi interesu ogólnego i jest środkiem adekwatnym do jego osiągnięcia. Przekazywanie określonych danych osobowych pasażerów lotniczych, a także ich zatrzymywanie ma bowiem umożliwić porównanie tych danych z określonymi wcześniej kryteriami oceny bądź bazami danych, tak aby zidentyfikować osoby dotąd nieznane organom ścigania. Niemniej jednak przepisy dotyczące tych kryteriów oceny i baz danych, a także zatrzymywania danych PNR przez okres pięciu lat nie spełniają wymogu niezbędności ingerencji. Regulacje te nie wprowadzają

[82] Art. 12 dyrektywy.

żadnego rozróżnienia w zależności od tego, których pasażerów to dotyczy, pozwalając zatem na zatrzymywanie danych PNR wszystkich pasażerów lotniczych. Innymi słowy, ustawodawca nie ograniczył ich w sposób jasny i precyzyjny do tego, co ściśle konieczne, powodując niezgodność wskazanych rozwiązań z art. 7, art. 8 oraz z art. 52 ust. 1 KPP. Można zatem się spodziewać, że przedmiotowa dyrektywa zostanie zbadana w najbliższym czasie przez TSUE.

Bibliografia

Blasi Casagran C., *The Future EU PNR System: Will Passenger Data be Protected?*, "European Journal of Crime, Criminal Law and Criminal Justice", No. 3/2015.

De Hert P., Papakonstantinou V., *Repeating the Mistakes of the Past Will Do Little Good for Air Passengers in the EU: The Comeback of the EU PNR Directive and a Lawyer's Duty to Regulate Profiling*, "New Journal of European Criminal Law", No. 2/2015.

Granger M, Irion K., *The Court of Justice and the Data Retention Directive in Digital Rights Ireland: Telling Off the EU Legislator and Teaching a Lesson in Privacy and Data Protection*, "European Law Review", No. 6/2014,

Kaunert C., Leonard S., McKenzie A., *The social construction of an EU interest in counter-terrorism: US influence and internal struggles in the cases of PNR and SWIFT*, "European Security", No. 4/2012.

Lowe D., *The European Union's Passenger Name Record Data Directive 2016/681: Is it Fit for Purpose?*, "International Criminal Law Review", No. 1/2017.

Rizer A., *Dog Fight: Did The International Battle Over Airline Passenger Name Records Enable The Christmas-day Bomber?*, "Catholic University Law Review", No. 1/2010.

Van Wasshnova M.R., *Data Protection Conflicts Between the United States and the European Union in the War on Terror: Lessons Learned from the Existing System Of Financial Information Exchange*, "Case Western Reserve Journal of International Law", No. 3/2007.

Vavoula V., *'I Travel, therefore I Am a Suspect': an overview of the EU PNR Directive*, 26.10.2016 r., http://eumigrationlawblog.eu/i-travel-therefore-i-am-a-suspect-an-overview-of-the-eu-pnr-directive/ (dostęp 6.06.2017).

Słowa kluczowe: dane PNR, prawa podstawowe, przetwarzanie danych PNR, zasada proporcjonalności, bezpieczeństwo publiczne

Key words: PNR Data, Fundamental Rights, Principle of Proportionality, Processing of PNR, Public Security

Directive (EU) 2016/681 of the European Parliament and of the Council on the Use of Passenger Name Record (PNR) Data – An Adequate Mean to Fight with Terrorism and Serious Crime or a Mass Surveillance Tool?

Abstract

On 28 April 2016 the Directive (EU) 2016/681 of the European Parliament and of the Council on the use of passenger name record (PNR) data for the prevention, detection, investigation and prosecution of terrorist offences and serious crime was adopted by the 28 Member States. Regulating this complex issue, European legislator has been obliged to strike a "fair balance" between the objective of combating terrorism and serious crime and the objective of protecting personal data and respecting the private life of the passengers. The aim of this paper is to analyse the provisions which apply to the processing of PNR data in the light of the principle of proportionality.