FUNDACJA PANOPTYKON

Warszawa, 28 listopada 2017 r.

Uwagi Fundacji Panoptykon[1] w sprawie projektu ustawy o przetwarzaniu danych dotyczących przelotu pasażera[2]

Projekt ustawy o przetwarzaniu danych dotyczących przelotu pasażera (dalej: **projekt**) stanowi implementację do prawa polskiego dyrektywy Parlamentu Europejskiego i Rady 2016/681 z 27 kwietnia 2016 r. 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 i ich ścigania (dalej: **dyrektywa**). W związku z tym, projekt należy oceniać tak w kontekście dyrektywy, jak i – w zakresie, w jakim dyrektywa przyznaje państwom członkowskim swobodę wyboru środków zmierzających do osiągnięcia jej celu – w kontekście całego systemu prawa Unii Europejskiej i wynikających z niego zasad.

Projekt dyrektywy został po raz pierwszy zaprezentowany przez Komisję Europejską w 2011 r., ale prace nad nim zostały porzucone w 2013 r. po odrzuceniu go przez Komisję Parlamentu Europejskiego ds. Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE), zdaniem której projekt stanowił poważne zagrożenie dla praw człowieka. Prace nad dyrektywą wznowiono w listopadzie 2014 r. i – w reakcji na zamach terrorystyczny na siedzibę redakcji francuskiego magazynu Charlie Hebdo ze stycznia 2015 r. – przeprowadzone zostały w tempie ekspresowym, mimo poważnych wątpliwości co do skuteczności i proporcjonalności przewidzianych środków w kontekście zapobiegania terroryzmowi i poważnym przestępstwom oraz zarzutów wprowadzenia nieuzasadnionych ograniczeń praw podstawowych[3].

Uwagi ogólne

Celem wdrażanej 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 (motyw 5 dyrektywy). Jednocześnie, dyrektywa stanowi niezwykle daleko idącą ingerencję w prawo do prywatności ogromnej liczby osób – dotknie ona miliony pasażerów podróżujących samolotem z i do Unii Europejskiej oraz – jeśli postanowią tak poszczególne państwa członkowskie – pomiędzy państwami członkowskimi. Zgodnie z motywem 22, przy stosowaniu dyrektywy należy zapewnić pełne poszanowanie praw podstawowych, prawa do prywatności i zasady proporcjonalności.

W tym kontekście, niezwykle istotne przy implementacji dyrektywy jest zatem zapewnienie przez projektodawcę spójności polskiej ustawy z całością systemu prawnego Unii Europejskiej,

[1] Stanowisko przygotowane przez Karolinę Iwańską.
[2] Projekt z dnia 14 listopada 2017 r.
[3] Por. np. Opinia 5/2015 Europejskiego Inspektora Ochrony Danych 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, pełny tekst w języku angielskim dostępny online: https://edps.europa.eu/sites/edp/files/publication/15-09-24_pnr_en.pdf.

a zwłaszcza z Kartą Praw Podstawowych UE, która stanowi gwarancję poszanowania praw człowieka w procesie stosowania prawa unijnego.

Projektodawca powinien więc przyjąć rozwiązania, które uwzględnią sposób interpretacji Karty Praw Podstawowych przedstawiony przez Trybunał Sprawiedliwości Unii Europejskiej w opinii z 26 lipca 2017 r. w sprawie zgodności z prawem unijnym projektu umowy między Kanadą a Unią Europejską dotyczącej przekazywania danych dotyczących przelotu pasażera z Unii do Kanady[4]. Projekt umowy umożliwiał przekazywanie danych PNR z Unii Europejskiej do Kanady (dotyczył zatem analogicznych kwestii co dyrektywa) oraz zawierał wiele zbieżnych z dyrektywą postanowień dotyczących przekazywania danych, m.in. w przypadku kategorii przekazywanych danych oraz okresu ich retencji. W opinii Trybunał uznał, że projekt umowy jest niezgodny z Kartą Praw Podstawowych m.in. w zakresie, w którym pozwala na przechowywanie przez okres 5 lat danych pasażerów, którzy nie budzili podejrzeń w momencie ich weryfikacji przez organy państwa, jak również poprzez nieprecyzyjne określenie kategorii danych PNR.

Obie wyżej wspomniane kwestie, które Trybunał uznał za niezgodne z Kartą Praw Podstawowych, zostały podobnie uregulowane w dyrektywie. Na trudność pogodzenia tych postanowień z opinią Trybunału zwróciła uwagę Służba Prawna Rady w nocie z 7 września 2017[5]. Potrzeba nowelizacji dyrektywy w świetle opinii Trybunału została wyrażona przez ekspertów[6], a rozmowy o konsekwencjach opinii dla dyrektywy toczą się również na szczeblu Komisji. Funkcjonowanie w obrocie prawnym aktu niezgodnego z Kartą Praw Podstawowych powoduje wysokie prawdopodobieństwo unieważnienia lub zmiany tego aktu. Polski projektodawca powinien zatem – w dbałości o spójność i stabilność prawa – podjąć wszelkie możliwe działania zmierzające do uniknięcia wprowadzenia do polskiego prawa uregulowań niezgodnych z prawami podstawowymi Unii.

Niezależnie od tego, poniżej przedstawiamy uwagi do konkretnych propozycji, które znalazły się w projekcie.

Uwagi szczegółowe

1. Zastosowanie ustawy do lotów wewnątrzunijnych

Ustawodawca unijny w art. 2 dyrektywy przyznał państwom członkowskim swobodę w zakresie zastosowania jej postanowień również do lotów odbywających się wewnątrz Unii Europejskiej. Polski projektodawca zdecydował się skorzystać z tej możliwości, definiując w art. 2 pkt 7 projektu lot PNR jako lot, podczas którego nastąpiło przekroczenie granicy państwowej, a start lub lądowanie statku powietrznego następuje na terytorium Polski. Z uzasadnienia wynika, że decyzja o rozszerzeniu zastosowania projektu również do lotów między państwami członkowskimi została podjęta w wyniku uzgodnień międzyresortowych.

Projektodawca – mając możliwość samodzielnego zdecydowania o zakresie zastosowania planowanej regulacji – wybrał opcję, która stanowi poważną ingerencję w prawa podstawowe i która doprowadzi do objęcia programem masowego zbierania i analizowania danych osobowych ogromnej liczby osób, zarówno obywateli Polski, jak i obywateli innych państw członkowskich oraz państw trzecich.

[4] Opinia 1/15 Trybunału Sprawiedliwości Unii Europejskiej z 26 lipca 2017 r.
[5] Nota informacyjna Służby Prawnej Rady z 7 września 2017 r., 11931/17.
[6] R. Bossong, *Passenger Name Records – from Canada back to the EU,* dostępny online: http://verfassungsblog.de/passenger-name-records-from-canada-back-to-the-eu/

Uważamy, że w zakresie, w jakim projektodawca nie jest ściśle związany postanowieniami dyrektywy, powinien on wybrać takie rozwiązanie, które będzie stanowiło mniejsze ograniczenie dla praw obywatelskich. Rozszerzenie stosowania projektowanych przepisów na loty wewnątrzunijne doprowadzi do gromadzenia nieporównywalnie większej liczby danych PNR niż gdyby zachowane zostały wyłącznie wymogi nałożone dyrektywą. Oznacza to, że do JIP co roku trafiać będą dane ok. 30 mln pasażerów polskich lotnisk[7] (loty poza Unię Europejską stanowią niewielki ułamek wszystkich połączeń[8]). Dane te pozostaną w bazie przez okres 5 lat, a dostęp do nich będą mogły uzyskać służby, a nawet organy innych państw członkowskich i państw trzecich. Rozszerzenie stosowania projektu na loty wewnątrzunijne, biorąc pod uwagę podnoszoną przez ekspertów i właściwe instytucje nieskuteczność i nieproporcjonalność zbierania danych PNR w walce z terroryzmem i poważną przestępczością, jest nieuzasadnionym ograniczeniem praw obywatelskich.

2. Inspektor ochrony danych w JIP

Dyrektywa w art. 5 ust. 2 stanowi, że państwa członkowskie udostępniają inspektorom ochrony danych powoływanych przez JIP środki umożliwiające im wykonywanie w sposób skuteczny i niezależny obowiązków i zadań dla niego przewidzianych (monitorowanie przetwarzania danych PNR i stosowanie odpowiednich gwarancji). Tymczasem, zgodnie z art. 48 ust. 2 projektu, w zakresie wykonywania swoich zadań inspektor podlega bezpośrednio Komendantowi Głównemu Straży Granicznej.

Uważamy, że taka konstrukcja nie spełnia wymogu niezależności inspektora przewidzianego w dyrektywie. Nawet jeśli projektodawca zdecyduje się utrzymać model funkcjonowania inspektora wewnątrz struktur Straży Granicznej, powinien przewidzieć gwarancje niezależnego sprawowania obowiązków. Za środki zapewniające zwiększenie niezależności inspektora można uznać np. wprowadzenie kadencyjności i zakaz odwołania inspektora przed upływem kadencji.

Z uwagi na wagę wykonywanych zadań, zasadne jest również podwyższenie wymagań przewidzianych wobec kandydatów na inspektora. Kryteria zawarte w art. 48 ust. 2 projektu są określone w sposób bardzo ogólny („osoby posiadające wiedzę i doświadczenie w zakresie nadzoru nad przetwarzaniem danych"). Projektodawca powinien doprecyzować, że inspektorem może zostać wyłącznie osoba posiadająca wyższe wykształcenie prawnicze, charakteryzująca się wyróżniającą się wiedzą w zakresie nadzoru nad przetwarzaniem danych, zwłaszcza w instytucjach publicznych, potwierdzoną wieloletnim doświadczeniem (postulujemy okres min. 5 lat).

3. Kategorie danych PNR

Wykaz kategorii danych, do których przekazywania będą zobowiązani przewoźnicy lotniczy znajduje się w Załączniku nr 1 do projektu. Wśród wymienionych kategorii, poważne wątpliwości budzą ujęte w pkt. 12 uwagi ogólne, a także wszelkie zebrane dane pasażera

---

[7] Urząd Lotnictwa Cywilnego, *Liczba obsłużonych pasażerów oraz wykonanych operacji w ruchu krajowym i międzynarodowym – regularnym i czarterowym w latach 2014-2016*, listopad 2017, opracowanie dostępne online: http://www.ulc.gov.pl/_download/regulacja_rynku/statystyki/IV_kw_2016/wg_portow_lotniczych-2016kw4_v2.pdf.

[8] Urząd Lotnictwa Cywilnego, *Liczba pasażerów obsłużonych w polskich portach lotniczych według krajów w międzynarodowym ruchu regularnym w czwartym kwartale 2015 i 2016 roku,* listopad 2017, opracowanie dostępne online: http://www.ulc.gov.pl/_download/regulacja_rynku/statystyki/IV_kw_2016/wg_krajow_regularne-2016kw4_v2.pdf.

przekazane przed podróżą ujęte w pkt. 17. Kategorie te określone zostały w sposób niewystarczająco precyzyjny. Na fakt ten zwrócił uwagę Trybunał Sprawiedliwości we wspomnianej we wstępie opinii dotyczącej umowy Unii z Kanadą. Ponieważ kategorie danych zostały w umowie sformułowane w sposób identyczny jak w dyrektywie, uwagi Trybunału dotyczące zgodności tych postanowień z prawami podstawowymi powinny zostać wzięte pod uwagę przez projektodawcę w celu uniknięcia naruszenia Karty Praw Podstawowych w związku z implementacją dyrektywy.

Projektodawca powinien zatem doprecyzować te kategorie w taki sposób, aby zagwarantować, że przekazywane dane nie obejmą danych wrażliwych. Doprecyzowanie może mieć charakter negatywny, tj. może polegać na dodaniu w nawiasie kategorii informacji, które nie powinny być przekazywane, np. dotyczących wyboru posiłku na pokładzie, co może pośrednio wskazywać na wyznanie pasażera, czy kwestii skorzystania przez pasażera z usług dodatkowych, które mogą sugerować stan zdrowia. Doprecyzowanie tych kategorii powinno znaleźć się w projekcie niezależnie od przewidzianego w art. 15 ust. 4 wymogu usunięcia danych wrażliwych, gdyby trafiły one do JIP. Z uwagi bowiem na wysokie sankcje łączące się z niewłaściwym wykonaniem obowiązków przez przewoźników (np. przekazaniem danych niekompletnych), istnieje wysokie ryzyko, że przewoźnicy, w celu uchronienia się przed sankcjami, będą przekazywali wszelkie zgromadzone dane, nawet jeśli są one danymi wrażliwymi. Precyzyjne wskazanie kategorii danych PNR i wyłączenie z katalogu konkretnie wskazanych danych pozwoli zminimalizować to ryzyko.

4. Przekazywanie danych PNR właściwym organom

- **Katalog właściwych organów**

Dyrektywa w art. 7 ust. 2 stanowi, że organami uprawnionymi do występowania do JIP z wnioskiem o dane PNR lub wyniki ich przetwarzania są organy właściwe do zapobiegania przestępstwom terrorystycznym lub poważnym przestępstwom, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania.

W katalogu właściwych organów przedstawionym przez projektodawcę w art. 28 projektu ujęte zostały dwa organy, które nie spełniają warunków przewidzianych w dyrektywie – Szef Agencji Wywiadu oraz Szef Służby Wywiadu Wojskowego. Zadaniem tych organów jest przede wszystkim rozpoznawanie zagrożeń. Swoje zadania służby te realizują poza granicami Polski[9], a realizacja czynności operacyjno-rozpoznawczych przez te służby na terenie kraju odbywa się wyłącznie za pośrednictwem odpowiednio Szefa Agencji Bezpieczeństwa Wewnętrznego i Szefa Służby Kontrwywiadu Wojskowego[10]. W związku z tym, nie jest zasadne uwzględnianie tych służb w katalogu organów, które mogą zwracać się bezpośrednio do JIP z wnioskiem o przekazanie danych PNR.

- **Wymogi formalne wniosku o przekazanie danych**

Przekazywanie danych PNR do właściwych organów odbywa się na wniosek. Projektodawca nie wymienił w sposób pozytywny wymogów, jakie powinien spełniać wniosek właściwego organu,

[9] Por. art. 6 ust. 2 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i art. 6 ust. 2 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

[10] Por. art. 6 ust. 3 ustawy z 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i art. 6 ust. 3 ustawy z 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego.

ograniczając się jedynie do wprowadzenia w art. 17 projektu przesłanek odmowy przekazania danych przez JIP. Uważamy za zasadne uwzględnienie również w art. 16 ust. 5 projektu wymogów dla wniosku właściwego organu, zgodnie z art. 6 ust. 2 lit. b dyrektywy.

5. Ujawnianie zdepersonalizowanych danych

Dyrektywa przewiduje, że po upływie 6 miesięcy od przekazania do JIP danych PNR, wszystkie dane poddane zostaną depersonalizacji. Jednym z kryteriów ujawnienia pełnych danych po upływie tego okresu jest – zgodnie z art. 12 ust. 3 lit. b dyrektywy – uzyskanie zgody organu wymiaru sprawiedliwości lub innego organu krajowego, który jest właściwy do ustalenia, czy warunki ujawnienia zostały spełnione, z zastrzeżeniem poinformowania o ujawnieniu inspektora ochrony danych w JIP oraz dokonaniu przez niego weryfikacji *ex post*.

Projektodawca w art. 25 ust. 2 pkt 2 zaproponował rozwiązanie, zgodnie z którym zgoda na ujawnienie zdepersonalizowanych danych mogłaby zostać wyrażona: w przypadku postępowania karnego – przez prokuratora lub sąd właściwy dla prowadzenia postępowania, a w przypadku wykonywanie czynności operacyjno-rozpoznawczych – właściwy organ prowadzący te czynności. Uważamy, że w tych sytuacjach zgodę powinien każdorazowo wyrazić organ, który w sposób obiektywny i niezależny oceni, czy spełnione zostały przesłanki ujawnienia danych, w szczególności, czy ujawnienie ich jest niezbędne w celu zapobiegania, zwalczania, wykrywania oraz ścigania przestępstw. W związku z tym, postulujemy, aby do ujawnienia zdepersonalizowanych danych każdorazowo wymagana była zgoda co najmniej prokuratora, również w przypadku wykonywania czynności operacyjno-rozpoznawczych. Jednocześnie uważamy, że najlepszym standardem byłoby wprowadzenie wymogu każdorazowego uzyskania zgody sądu.

Powierzenie tego zadania organom prowadzącym te czynności powoduje niezwykle wysokie ryzyko arbitralności przy ocenie niezbędności ujawnienia danych i jest niedopuszczalne w demokratycznym państwie prawnym. Wprowadzenie wymogu uzyskania zgody niezależnego organu jest konieczną gwarancją poszanowania praw osób, których dane miałyby zostać ujawnione oraz potrzebnym w demokratycznym państwie prawnym mechanizmem kontrolnym wobec pozyskiwania danych obywateli przez służby.

Z kolei zgodnie z art. 34 ust. 1 pkt 2 projektu, do przekazania zdepersonalizowanych danych do JIP pozostałych państw członkowskich i organów państw trzecich niezbędna jest zgoda prokuratora okręgowego właściwego miejscowo ze względu na siedzibę JIP. Uważamy za nieuzasadnione i niewskazane rozróżnianie organu właściwego do potwierdzenia, że warunki ujawnienia zdepersonalizowanych danych zostały spełnione, w zależności od tego, czy dane te mają być ujawnione polskim służbom czy JIP państw członkowskich. W obu przypadkach właściwy do wydania zgody powinien być co najmniej prokurator, a najlepiej – niezależny sąd.

***

Podsumowując, Fundacja Panoptykon postuluje implementację dyrektywy w sposób spójny z Kartą Praw Podstawowych i jej interpretacją przez Trybunał Sprawiedliwości UE, jak również ograniczenie zastosowania ustawy wyłącznie do danych PNR pasażerów lotów pozaunijnych. Postulujemy także wzmocnienie niezależności inspektora ochrony danych w JIP, doprecyzowanie kategorii przekazywanych danych, jak również wymogów, jakie powinien spełnić wniosek właściwych organów. Apelujemy także o wprowadzenie wymogu uzyskania uprzedniej zgody niezależnego organu w przypadku konieczności ujawnienia danych zdepersonalizowanych.