



PRZEKAZYWANIE DANYCH PASAŻERÓW LINII LOTNICZYCH POROZUMIENIE UNII EUROPEJSKIEJ Z KANADĄ W SPRAWIE DANYCH PNR

Od kilku lat dane pasażerów linii lotniczych (*Passenger Name Records*, PNR) są wykorzystywane przez organy ścigania na potrzeby walki z terroryzmem i poważną przestępczością. Dane PNR wszystkich pasażerów europejskich linii lotniczych oraz samolotów lecących z i do Europy trafiają do odpowiednich służb kanadyjskich jeszcze zanim samolot wystartuje. Na tej podstawie weryfikuje się, czy wśród pasażerów znajdują się osoby mogące stanowić zagrożenie dla bezpieczeństwa. Pierwsze europejskie porozumienie z Kanadą w sprawie przekazywania danych PNR zostało podpisane w 2006 roku. Podobne umowy obowiązują również w stosunkach z USA i Australią. Wszystkie budzą poważne kontrowersje, ponieważ ingerują w prawa obywatelskie, w szczególności w prawo do prywatności i ochrony danych osobowych.

CZYM SĄ DANE PNR?

PNR to dane o pasażerach zbierane zwyczajowo przez linie lotnicze. Zaliczają się do nich: imię, nazwisko, adres e-mail, numer telefonu, trasa podróży, forma płatności za bilet, numer karty kredytowej, informacja o bagażu. Gromadzone są także informacje o rezerwacjach hotelowych, wynajmie samochodu czy zakupie biletu kolejowego, jeśli tylko strona linii lotniczych oferuje taką możliwość. Dane PNR mogą zawierać także wrażliwe informacje, takie jak preferencje dotyczące posiłku serwowanego na pokładzie samolotu (np. koszerne, halal, wegetariański czy bez wieprzowiny) albo fakt rezerwowania pokoju z podwójnym łóżkiem (co może zdradzać relacje intymne).

JAKIE WZBUDZA TO KONTROWERSJE?

- Nie ma dowodów na to, że masowe przekazywanie danych pasażerów linii lotniczych pozwala zmniejszyć zagrożenie atakami terrorystycznymi, natomiast w istotny sposób ogranicza prywatność pasażerów i stwarza ryzyko poważnych nadużyć. Samo już więc gromadzenie i przekazywanie danych PNR stanowi naruszenie zasad niezbędności i proporcjonalności zawartych w Karcie Praw Podstawowych.
- W praktyce wykorzystywanie danych PNR oznacza automatyczne traktowanie każdego podróżnego jako potencjalnie podejrzanego o terroryzm czy popełnienie poważnego przestępstwa. Na podstawie ograniczonych danych z systemów rezerwacyjnych wyciągane są kontrowersyjne wnioski, a na czarnej liście można trafić przez pomyłkę lub przypadek (np. w Wielkiej Brytanii w wyniku analizy danych PNR na czarnych listach znaleźli się m.in. wegetarianie, osoby wykupujące rezerwacje *last minute* i pasażerowie podróżujący w jedną stronę).
- Umowa w sprawie przekazywania danych PNR pozwala na wykorzystywanie danych wrażliwych. Dodatkowo nie został wprowadzony zakaz automatycznego profilowania osób na podstawie danych PNR, co może prowadzić do dyskryminacji i utrwalania krzywdzących stereotypów.
- Porozumienie PNR nie przewiduje realnych gwarancji ochrony praw obywateli UE w Kanadzie. Teoretycznie mamy prawo do informacji o zgromadzonych na nasz temat danych, ale amerykańskie organy nie mają obowiązku takiej informacji udzielić. Podobnie jest z prawem do skorygowania

zgromadzonych informacji. Brakuje także nadzoru ze strony niezależnego organu nad przetwarzaniem danych przez służby kanadyjskie.

- Dane pasażerów lecących z Europy mają być przechowywane w Kanadzie przez 5 lat. To dłużej niż przewidywała tzw. dyrektywa retencyjna (dane telekomunikacyjne miały być przechowywane przez operatorów na potrzeby walki z poważną przestępczością maksymalnie przez 2 lata).
- Gwarancje dotyczące maksymalnego czasu przechowywania danych i obowiązku ich usunięcia po upływie tego czasu są pozorne i nieegzekwowalne w praktyce.
- Nie wiadomo, które dokładnie organy mają dostęp do danych przekazywanych z Unii Europejskiej – projekt porozumienia mówi enigmatycznie o „właściwych organach kanadyjskich”.

Analogiczne zastrzeżenia zostały podniesione także przez Europejskiego Inspektora Ochrony Danych Osobowych oraz Grupę roboczą ds. ochrony osób fizycznych w zakresie przetwarzania danych osobowych (tzw. Grupa Robocza art. 29). Co więcej, mechanizm przetwarzania danych PNR jest bardzo podobny do gromadzenia danych telekomunikacyjnych przez operatorów na potrzeby walki z przestępczością. Umożliwiający to przepisy tzw. dyrektywy retencyjnej zostały niedawno unieważnione przez Trybunał Sprawiedliwości Unii Europejskiej (TSUE). TSUE uznał, że prewencyjne gromadzenie danych o wszystkich połączeniach telekomunikacyjnych i ich udostępnianie organom ścigania bez kontroli sądu stanowi nieproporcjonalne naruszenie praw i wolności obywatelskich.

W związku z tymi poważnymi wątpliwościami uważamy, że Trybunał Sprawiedliwości Unii Europejskiej powinien rozstrzygnąć ostatecznie, czy projekt porozumienia w sprawie przekazywania danych PNR między Unią Europejską a Kanadą spełnia wymogi stawiane przez Kartę Praw Podstawowych.

O Fundacji Panoptykon

Fundacja Panoptykon powstała w kwietniu 2009 r. Jej celem jest działanie na rzecz ochrony praw człowieka w kontekście rozwoju „społeczeństwa nadzorowanego” – współczesnych form kontroli i nadzoru nad społeczeństwem. W obszarze zainteresowania Fundacji znajdują się takie zagadnienia jak: powstawanie i rozbudowa baz danych, rozwój monitoringu wizyjnego, retencja danych telekomunikacyjnych, wykorzystywanie technologii biometrycznych, uprawnienia służb specjalnych, techniki nadzoru nad pracownikami, praktyki kontroli przepływu informacji w Internecie.

