

Jakie dane z linii lotniczych trafią w ręce służb?

14 lipca 2015

W Brukseli trwają intensywne prace nad przyjęciem dyrektywy, która zobowiąże linie lotnicze do przekazywania służbom szczegółowych danych (tzw. Passenger Name Records) o wszystkich pasażerach podróżujących z lub do Unii Europejskiej. Każdy pasażer będzie traktowany jak potencjalny terrorysta – pod tym kątem będzie tworzony i analizowany jego profil. Jakie dane trafią w ręce służb i w jaki sposób będą wykorzystywane? Kto i na jakiej zasadzie będzie mieć do nich dostęp? Jakie to może mieć konsekwencje dla każdego z nas i czy faktycznie zwiększy bezpieczeństwo? Przedstawiamy założenia nowego systemu walki z terroryzmem i poważną przestępczością, opartego na analizie danych PNR.

JAKIE DANE NA NASZ TEMAT BĘDĄ ZBIERANE?

W nowym systemie mają być przetwarzane dane wszystkich pasażerów podróżujących z lub do Unii Europejskiej. Jeśli zdecydujemy się na wakacje w Egipcie czy Turcji albo podróż służbową poza granice UE, nasz profil (w żargonie zwany „rekordem PNR”) trafi do specjalnej, krajowej bazy danych. Zgodnie z projektem dyrektywy w skład tego profilu wejdą:

- dane osobowe pasażera (imię, nazwisko, adres, numer dokumentu etc.),
- szczegółowe dane o samym locie (data, godzina, trasa, typ maszyny),
- dane osoby, która dokonała rezerwacji,
- forma płatności (łącznie z numerem wykorzystanej karty kredytowej),
- specjalne życzenia pasażera (w tym informacja o poruszaniu

się na wózku lub ciąży),

– numer miejsca w samolocie,

– numer biletu,

– numer przypisany w programie lojalnościowym,

– informacje o nadanym lub zabranym na pokład bagażu,

– adnotacje o niestawieniu się na lot, zmianie miejsca czy nietypowym lub irytującym zachowaniu pasażera (wprowadza je obsługa linii lotniczych).

GDZIE TRAFIĄ DANE I KTO BĘDZIE MIAŁ DO NICH DOSTĘP?

Zgodnie z projektem dyrektywy linie lotnicze będą przekazywać dane swoich pasażerów do nowo utworzonych jednostek – tzw. Passenger Information Units (PIU). Trudno przewidzieć, jak taka jednostka zostanie zorganizowana w Polsce: może mieć niezależny charakter, ale może też działać w ramach innej formacji – policji czy nawet ABW. Dane będą przesyłane dwa razy: w przedziale 48-24 godz. przed odlotem oraz zaraz po zamknięciu bramek, kiedy lista pasażerów jest już ostateczna. Czas ma znaczenie, ponieważ podstawowym zadaniem PIU ma być analizowanie danych w czasie rzeczywistym i przekazywanie odpowiednim organom (np. policji lub straży granicznej) alertów, jeśli profil konkretnego pasażera wyda się analitykom podejrzany.

Kolejnym zadaniem PIU ma być udostępnianie danych innym uprawnionym organom na ich wyraźną i uzasadnioną prośbę. Listę takich organów każde państwo członkowskie stworzy według własnej oceny, co daje pewne pole do manewru. W praktyce dane PNR z pewnością trafią do polskiej policji i każdej służby, która w swoich zadaniach ma walkę z terroryzmem lub poważną przestępczością.

Niezależnie od reagowania na zapytania i wnioski od uprawnionych organów (związanych z konkretnymi sprawami), PIU

będzie też przeprowadzać własne analizy na podstawie zbieranych danych (np. trendów w międzynarodowej przestępczości) i dzielić się wnioskami z odpowiednimi służbami.

JAK DŁUGO DANE BĘDĄ PRZETWARZANE?

Przez pierwsze 30 dni dane zebrane przez PIU będą przetwarzane i przekazywane innym organom (jeśli o to zawnioskują) w pełnym zakresie, ze wszystkimi szczegółami identyfikującymi pasażerów. Po upływie tego okresu projekt dyrektywy przewiduje tzw. maskowanie, czyli wydzielenie danych bezpośrednio identyfikujących pasażera (np. imię i nazwisko, numer dokumentu) do oddzielnej bazy. Ma to zwiększyć ochronę danych i zabezpieczyć prawa pasażerów. Ponowne skojarzenie danych bezpośrednio identyfikujących pasażera z jego pełnym profilem będzie wymagało zgody szefa PIU. Tak „spseudonimizowane” profile PNR będą przetwarzane jeszcze przez 5 lat i gdy zajdzie tak potrzeba przekazywane odpowiednim służbom – najdłużej, bo aż przez cały ten okres, będzie można sięgnąć po PNR na potrzeby walki z terroryzmem.

CZEMU TAK NAPRAWDĘ MA SŁUŻYĆ SYSTEM PNR?

Oficjalnie system PNR ma służyć zapobieganiu, wykrywaniu, dochodzeniu i ściganiu terroryzmu oraz innych poważnych przestępstw, szczególnie o charakterze międzynarodowym (w grę wchodzi handel ludźmi czy handel narkotykami). Jednak Komisja Europejska nie wykazała, w jaki sposób dane z systemów rezerwacyjnych miałyby pomóc w tak trudnych sprawach. Są za to inne cele, które podobne systemy – już działające np. w Wielkiej Brytanii, USA czy Brazylii – realizują z pewnym powodzeniem. Dobrym przykładem jest namierzanie tras nielegalnych migracji czy osób, które omijają przepisy wizowe albo podejrzanie często (w oczach fiskusa) przekraczają przez granicę w celach zarobkowych lub na bezcłowe zakupy. Trudno przewidzieć, czy – kiedy już system powstanie – Unia Europejska też nie pójdzie tą drogą.

NA CZYM POLEGA PROBLEM?

System PNR to flagowy przykład polityki opartej na przekonaniu, że zebranie kolejnych kategorii danych zwiększy nasze bezpieczeństwo. Nikt jeszcze jednak nie wykazał, w jaki sposób analiza bardzo typowych i podstawowych danych, które są zbierane przez linie lotnicze, pomoże w walce z terroryzmem czy poważną przestępczością. Z drugiej strony, znamy wiele argumentów – w tym formułowanych przez byłych analityków służb specjalnych – na to, że sama dostępność danych nie pomaga w pracy służb. Kluczowa jest ich inteligentna analiza i umiejętność precyzyjnego definiowania celów. A do tego typu pracy prewencyjne zbieranie danych o wszystkich podróżujących nie jest potrzebne: wystarczyłoby sprawne wykorzystywanie danych PNR w konkretnych sprawach, np. kiedy już wiadomo, że na danej trasie dzieje się coś niepokojącego, albo że poszukiwana osoba próbuje przekroczyć granicę. Takie działanie jest możliwe już dziś i nie wymaga nowego prawa ani nowej bazy danych.

Grozi nam zatem utopienie potężnych publicznych środków w systemie, który nie jest niezbędny, a wręcz może być szkodliwy. Raz zebrane dane zaczynają żyć własnym życiem – trudno dziś przewidzieć, do jakich celów decydenci polityczni czy same służby zechcą je wykorzystać w przyszłości. Bardzo problematyczne mogą się też okazać analizy i alerty generowane przez PIU – szukając igły w stogu siana i profilując domniemyanych terrorystów na bazie podstawowych, typowych informacji, analitycy są skazani na olbrzymi margines błędu. Musimy się więc liczyć ze wzrostem liczby nieuzasadnionych zatrzymań na lotniskach, dziwnych pytań i rzucaniem bezpodstawnych podejrzeń poprzez takie działania jak wydzielenie do dodatkowej kontroli.

Wreszcie, jest duża szansa, że nowe prawo zostanie uznane za niezgodne z Kartą Praw Podstawowych UE i unieważnione, ale zajmie to lata i pochłonie dodatkowe środki. Taki wyrok Trybunał Sprawiedliwości UE już wydał w odniesieniu do

dyrektywy, która nakazywała – również na potrzeby walki z terroryzmem i poważną przestępczością – prewencyjne przechowywanie i przekazywanie danych telekomunikacyjnych przez operatorów. Dyrektywa tworząca system PNR jest oparta na tej samej logice i stwarza analogiczne problemy, jeśli chodzi o przestrzeganie praw podstawowych obywateli. Tworząc nowe prawo Unia Europejska nie powinna powtarzać starych błędów.

Projekt dyrektywy o systemie PNR, przygotowany przez Komisję Europejską, jest obecnie procedowany w Parlamencie Europejskim. W najbliższą środę, 15 lipca, będzie nad nim dyskutować i głosować Komisja Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych (LIBE). Z polskich posłów zasiadają w niej: Barbara Kudrycka, Michał Boni, Marek Jurek (zastępstwo), Jarosław Kalinowski (zastępstwo), Róża Thun (zastępstwo) i Kazimierz Ujazdowski (zastępstwo). Głosowanie plenarne odbędzie się najprawdopodobniej na jesieni.

Autorstwo: Katarzyna Szymielewicz

Źródło: Panoptikon.org