Revista Europea de Derecho de la Navegación Marítima y Aeronáutica

ISSN versión electrónica: 2386-8902

DYREKTYWA PARLAMENTU EUROPEJSKIEGO I RADY UE NR 2016/681 Z 27 KWIETNIA 2016 R. W SPRAWIE WYKORZYSTYWANIA DANYCH DOTYCZACYCH PRZELOTU PASAZERA (DANYCH PNR-PASSENGER NAME RECORD) W KONTEKSCIE BEZPIECZENSTWA PASAZERÓW ORAZ ICH PRYWATNOSCI

Tomasz BALCERZAK

Resumen: Comenta Tomasz Balcerzak un decreto del Parlamento europeo sobre navegación aeronáutica nº 2016/681, con una serie de consideraciones colaterales relacionadas tanto con con la tripulación como con el pasaje aéreo. Aborda también asuntos de seguridad aeronáutica.

Palabras clave: Transporte aéreo, Seguridad, Parlamento europeo, Derecho aeronáutico, Gran Bretaña, Bélgica, Dinamarca, Francia, Países Bajos, Suecia.

Projekt dyrektywy w sprawie systemu przekazywania władzom informacji o pasażerach, czyli tzw. PNR (ang. Passenger Name Record), pojawił się już w 2011 r. Zgodnie z jego założeniami, linie lotnicze miałyby obowiązek przekazywać władzom dane osób wjeżdżających na terytorium Unii Europejskiej lub je opuszczających, a państwa członkowskie musiałyby stworzyć krajowe systemy danych pasażerów w oparciu o wspólne unijne zasady.

Zamach terrorystyczny na redakcję francuskiego magazynu satyrycznego Charlie Hebdo z 7 stycznia 2015 r. sprawił, że odżyła idea unijnej dyrektywy o wymianie danych osób podróżujących samolotami pasażerskimi. Premier Łotwy, przedstawiając w Parlamencie Europejskim priorytety łotewskiego przewodnictwa w UE, jako jeden z nich wymieniła potrzebę reaktywowania mechanizmów na rzecz zwalczania terroryzmu. Takim mechanizmem ma być m.in. skuteczna wymiana informacji pomiędzy wszelkimi służbami. O przyspieszenie prac nad wspólnym systemem wymiany informacji o pasażerach, podczas swojego pierwszego wystąpienia w Parlamencie Europejskim, apelował również Szef Rady Europejskiej. W niezbędność przekazywania danych wątpi jednak Europejski Inspektor Ochrony Danych, którego zdaniem, jeszcze nikt nie udowodnił, że taki system będzie stanowił skuteczną walkę z terroryzmem.

Swój system automatycznego zbierania i przekazywania danych ma już Wielka Brytania. Belgia, Dania, Francja, Holandia i Szwecja są w zaawansowanych fazach wprowadzania takich systemów u siebie. Jednak dla ich faktycznej efektywności niezbędne jest wprowadzenie wymiany tych informacji między państwami.

Umowa z 17 maja 2004r. zawarta pomiędzy Unią Europejską i Stanami Zjednoczonymi przewiduje, że każda linia lotnicza, która realizuje przeloty pasażerskie z lub do Stanów Zjednoczonych, musi zapewnić instytucji DHS (Department of Homeland Security)-Departamentowi Bezpieczeństwa Krajowego, elektroniczny dostęp do danych PNR, które są pobierane i przechowywane w systemach rezerwacji-odprawy danej linii lotniczej. Elektroniczne przekazywanie danych PNR przed przybyciem pasażerów do docelowego portu lotniczego na terenie Stanów Zjednoczonych względnie przed wyjazdem z USA, umożliwia władzom amerykańskim, poddanie pasażerów szybkiej i skutecznej analizie zagrożenia. Dane PNR pobrane przy przelotach pomiędzy Unią Europejską i USA przechowywane są przez instytucje DHS przez trzy lata i sześć miesięcy, chyba ze instytucja DHS zasięga konsultacji odnośnie określonych danych PNR. W tym przypadku instytucja DHS przechowuje dane PNR przez dalsze osiem lat. 27. wietnia 2016 r., 28 krajów członkowskich Unii Europejskiej przyjęło Dyrektywę Parlamentu Europejskiego i Rady UE nr 2016/681 w sprawie wykorzystywania danych dotyczących przelotu pasażera (danych PNR-Passenger Name Record), w celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania (Dz.Urz.UE L 119/132 z dnia 4 maja 2016 r.) Decyzja ta była poprzedzona wcześniejszymi pracami i aktami prawnymi w tym zakresie: 6 listopada 2007 r. Komisja Europejska przyjęła wniosek dotyczący decyzji ramowej Rady w sprawie wykorzystywania danych dotyczących rezerwacji pasażera (danych PNR) w celu egzekwowania prawa. Jednakże w związku z wejściem w życie w dniu 1 grudnia 2009 r. traktatu lizbońskiego2 wniosek Komisji, który nie został do tego dnia przyjęty przez Radę, stał się nieaktualny. W „Programie sztokholmskim – otwarta i bezpieczna Europa dla dobra i ochrony obywateli”3 zaapelowano do Komisji o przedłożenie wniosku dotyczącego wykorzystywania danych PNR w celu zapobiegania terroryzmowi i poważnej przestępczości, ich wykrywania, prowadzenia postepowań przygotowawczych w ich sprawie i ich ścigania. W komunikacie z dnia 21 września 2010 r. zatytułowanym „Globalne podejście do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim” Komisja przedstawiła kilka zasadniczych elementów polityki unijnej w tej dziedzinie. Dyrektywa Rady 2004/82/WE reguluje przekazywanie przez przewoźników lotniczych właściwym organom krajowym danych pasażera przekazanych przed podróżą (zwanych dalej „danymi API”-ang. Application Programming Interface)4 w celu poprawy kontroli granicznej i zwalczania nielegalnej imigracji.

Celem najnowszej dyrektywy UE jest, między innymi, zapewnienie bezpieczeństwa ogólnego, ochrona życia i bezpieczeństwa osób oraz stworzenie ram prawnych służących ochronie danych PNR w związku z ich przetwarzaniem przez właściwe organy.

Dyrektywa reguluje również wykorzystywanie danych PNR, między innymi poprzez porównanie danych PNR z danymi zawartymi w różnych bazach danych poszukiwanych osób i przedmiotów jako czynniki niezbędne do zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania, a tym samym do zwiększania bezpieczeństwa wewnętrznego, do zebrania dowodów, a – w odpowiednich przypadkach – do wykrycia współsprawców przestępstw i rozpracowania siatek przestępczych.

Sprawdzenie danych PNR będzie umożliwiało identyfikację osób, które przed dokonaniem takiego sprawdzenia nie były podejrzewane o udział w przestępstwach terrorystycznych lub w poważnej przestępczości i które powinny być poddane dalszemu sprawdzeniu przez właściwe organy. Dzięki wykorzystywaniu danych PNR będzie można reagować na zagrożenie przestępstwami terrorystycznymi i poważną przestępczością z innej perspektywy niż w przypadku przetwarzania innych kategorii danych osobowych. Jednakże aby ograniczyć przetwarzanie danych PNR do niezbędnego minimum, ustalanie i stosowanie kryteriów dokonywania sprawdzeń należy ograniczyć do przestępstw terrorystycznych i poważnej przestępczości, w przypadku których stosowanie takich kryteriów jest właściwe. Ponadto kryteria dokonywania sprawdzeń powinny zostać określone w taki sposób, by ograniczyć do minimum liczbę osób niewinnych błędnie zidentyfikowanych przez system.

Przewoźnicy lotniczy już zbierają i przetwarzają dane PNR swoich pasażerów do celów prowadzonej przez siebie działalności gospodarczej5. Nowa dyrektywa nie powinna nakładać na przewoźników lotniczych żadnych obowiązków dotyczących zbierania lub zatrzymywania jakichkolwiek dodatkowych danych pochodzących od pasażerów ani nie powinna nakładać na pasażerów żadnych obowiązków dotyczących dostarczania jakichkolwiek innych danych niż te, które już są dostarczane przewoźnikom lotniczym.

Niektórzy przewoźnicy lotniczy zatrzymują zebrane przez nich dane API jako część danych PNR, podczas gdy inni przewoźnicy tego nie czynią. Wykorzystywanie danych PNR wraz z danymi API stanowi wartość dodaną w zakresie pomocy państwom członkowskim w weryfikacji tożsamości osób, zwiększając tym samym przydatność wyników tych działań dla ścigania przestępczości i minimalizując ryzyko dokonywania sprawdzeń i prowadzenia postępowań przygotowawczych w stosunku do osób niewinnych. Ważne jest zatem zapewnienie, by przewoźnicy lotniczy, którzy zbierają dane API, przekazywali je bez względu na to, czy środki techniczne, za pomocą których zatrzymują dane API, są takie same jak w przypadku innych danych PNR.

W celu zapobiegania przestępstwom terrorystycznym i poważnej przestępczości, ich wykrywania, prowadzenia postępowań przygotowawczych w ich sprawie i ich ścigania istotne jest, by wszystkie państwa członkowskie ustanowiły przepisy nakładające na przewoźników lotniczych obsługujących loty pozaunijne obowiązek przekazywania zebranych danych PNR, w tym danych API. Państwa członkowskie powinny mieć również możliwość rozszerzenia tego obowiązku na przewoźników lotniczych obsługujących loty wewnątrzunijne. Przepisy te nie powinny naruszać dyrektywy 2004/82/WE. Przetwarzanie danych osobowych powinno być proporcjonalne do szczególnych celów dotyczących bezpieczeństwa, którym służy opisywana dyrektywa.

Definicja przestępstw terrorystycznych przyjęta na potrzeby nowej dyrektywy powinna być taka sama jak definicja w decyzji ramowej Rady 2002/475/WSiSW (Rada ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych). Definicja poważnej przestępczości powinna obejmować rodzaje przestępstw wymienione w załączniku II do tej dyrektywy6.

Dane PNR powinny być przekazywane do jednej wyznaczonej jednostki do spraw informacji o pasażerach (zwanej dalej „JIP") we właściwym państwie członkowskim, tak by zapewnić przejrzystość i ograniczyć koszty ponoszone przez przewoźników lotniczych. JIP może mieć swoje oddziały w jednym państwie członkowskim; państwa członkowskie mogą także wspólnie ustanowić jedną JIP. Państwa członkowskie powinny wymieniać między sobą informacje za pośrednictwem odpowiednich sieci wymiany informacji, aby ułatwiać dzielenie się informacjami i zapewnić interoperacyjność. Koszty związane z wykorzystywaniem, zatrzymywaniem i wymianą danych PNR powinny ponosić państwa członkowskie.

Wykaz danych PNR otrzymywany przez JIP należy sporządzać w taki sposób, by spełniał wymagania zarówno uzasadnionym potrzebom organów publicznych w związku z zapobieganiem przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywaniem, prowadzeniem postępowań przygotowawczych w ich sprawie i ich ściganiem, przyczyniając się tym samym do poprawy bezpieczeństwa wewnętrznego w Unii, jak również ochronie praw podstawowych, w szczególności prawa do prywatności i ochrony danych osobowych. W tym celu należy stosować wysokie standardy zgodnie z Kartą praw podstawowych Unii Europejskiej (zwaną dalej „Kartą praw podstawowych"), Konwencją o ochronie osób w związku z automatycznym przetwarzaniem danych osobowych (zwaną dalej „Konwencją nr 108") i Konwencją o ochronie praw człowieka i podstawowych wolności (zwaną dalej „Konwencją praw człowieka"). Wykaz taki nie powinien opierać się na rasie ani pochodzeniu etnicznym, na religii ani przekonaniach, na poglądach politycznych ani jakichkolwiek innych poglądach, na przynależności do związków zawodowych, stanie zdrowia, życiu seksualnym ani orientacji seksualnej danej osoby. Dane PNR powinny zawierać wyłącznie informacje dotyczące rezerwacji i tras podróży pasażerów, które umożliwią właściwym organom identyfikację pasażerów lotniczych stanowiących zagrożenie dla bezpieczeństwa wewnętrznego.

Dyrektywa przewiduje dwie metody przekazywania danych: metoda „pobierania", polegająca na tym, że właściwe organy państwa członkowskiego potrzebujące danych PNR mogą skorzystać z dostępu do systemu rezerwacji przewoźnika lotniczego i pobrać (ang. „pull") kopię potrzebnych danych PNR; oraz metoda „dostarczania", polegająca 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. Uznaje się, że metoda „dostarczania" zapewnia wyższy poziom ochrony danych i powinna być obowiązkowa dla wszystkich przewoźników lotniczych.

Zgodnie z założeniami nowej dyrektywy państwa członkowskie powinny podjąć wszelkie niezbędne środki, aby umożliwić przewoźnikom lotniczym wypełnianie obowiązków nałożonych na nich na jej podstawie. Wobec przewoźników lotniczych, którzy nie wypełniają obowiązków w zakresie przekazywania danych PNR, państwa członkowskie mogą przewidzieć skuteczne, proporcjonalne i odstraszające sankcje, w tym kary finansowe.

W założeniach do dyrektywy mówi się również o tym, że uwzględniając w pełni prawo do ochrony danych osobowych oraz prawo do niedyskryminacji, nie można podejmować wyłącznie na podstawie automatycznego przetwarzania danych PNR żadnych decyzji, które miałyby negatywne skutki prawne dla danej osoby lub znacząco wpływałyby na jej sytuację.

Ponadto, mając na uwadze art. 8 i 21 Karty praw podstawowych, żadna taka decyzja nie powinna nikogo dyskryminować ze względu na płeć, rasę, kolor skóry, pochodzenie etniczne lub społeczne, cechy genetyczne, język, religię lub przekonania, poglądy polityczne lub wszelkie inne poglądy, przynależność do mniejszości narodowej, majątek, urodzenie, niepełnosprawność, wiek lub orientację seksualną. Wyniki przetwarzania danych PNR nie powinny w żadnym przypadku być wykorzystywane przez państwa członkowskie jako powód do obejścia międzynarodowych zobowiązań wynikających z Konwencji z dnia 28 lipca 1951 r. dotyczącej statusu uchodźców, zmienionej protokołem z dnia 31 stycznia 1967 r.; wyniki te nie powinny być również wykorzystywane do odmawiania osobom ubiegającym się o azyl bezpiecznego i legalnego wjazdu na terytorium Unii w celu skorzystania z przysługującego im prawa do ochrony międzynarodowej.

Zgodnie z założeniami dyrektywy, państwa członkowskie powinny wymieniać otrzymywane dane PNR między sobą oraz z Europolem, jeżeli zostanie to uznane za niezbędne do zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywania, prowadzenia postepowań przygotowawczych w ich sprawie lub ich ścigania. JIP powinny, w stosownych przypadkach, przekazywać bezzwłocznie JIP w innych państwach członkowskich wyniki przetwarzania danych PNR w celu prowadzenia dalszego postępowania przygotowawczego.

Dyrektywa mówi również o tym, 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. Po upływie 6 miesięcy początkowego okresu zatrzymania, dane PNR powinny zostać poddane depersonalizacji poprzez maskowanie elementów danych, aby zapobiec ich nieproporcjonalnemu wykorzystywaniu. Po upływie początkowego okresu zatrzymania dostęp do pełnych danych PNR, które umożliwiają bezpośrednie zidentyfikowanie osoby, której dane dotyczą, powinien być możliwy wyłącznie po spełnieniu bardzo restrykcyjnych i ściśle określonych warunków, aby zapewnić jak najwyższy poziom ochrony danych.

Mając na uwadze prawo do ochrony danych osobowych, prawa osób, których dane dotyczą, odnoszące się do przetwarzania ich danych PNR, takie jak prawo dostępu do tych danych, ich poprawiania, usunięcia i ograniczania oraz prawo do odszkodowania i prawo do sądowych środków ochrony prawnej, powinny być zgodne zarówno z decyzją ramową 2008/977/WSiSW, jak również z wysokim poziomem ochrony przewidzianym w Karcie praw podstawowych i Konwencji praw człowieka.

Uwzględniając prawo pasażerów do uzyskania informacji o przetwarzaniu ich danych osobowych, państwa członkowskie powinny zapewnić, by pasażerowie otrzymywali w sposób łatwo dostępny i zrozumiały dokładne informacje na temat zbierania danych PNR, przekazywania ich do JIP oraz o prawach przysługujących im jako osobom, których dane dotyczą.

Przekazywanie danych PNR przez państwa członkowskie państwom trzecim powinno być dopuszczalne wyłącznie na podstawie oceny każdego indywidualnego przypadku i powinno odbywać się w pełnej zgodzie z przepisami ustanowionymi przez państwa członkowskie na podstawie decyzji ramowej 2008/977/WSiSW. Aby zapewnić ochronę danych osobowych, takie przekazywanie danych powinno podlegać dodatkowym wymogom dotyczącym celu przekazywania. Powinno ono także podlegać zasadom konieczności i proporcjonalności oraz wysokiemu poziomowi ochrony zapewnianemu przez Kartę praw podstawowych i Konwencję praw człowieka.

W związku z prawnymi i technicznymi różnicami w przepisach krajowych dotyczących przetwarzania danych osobowych, w tym danych PNR, przewoźnicy lotniczy spotykają się i będą się spotykać ze zróżnicowanymi wymogami co do rodzaju informacji, które należy przekazać, oraz co do warunków, zgodnie z którymi należy je dostarczać właściwym organom krajowym. Różnice te mogą utrudnić skuteczną współpracę między właściwymi organami krajowymi mającą na celu zapobieganie przestępstwom terrorystycznym lub poważnej przestępczości, ich wykrywanie, prowadzenie postępowań przygotowawczych w ich sprawie i ich ściganie. Niezbędnym jest zatem ustanowienie na poziomie unijnym wspólnych ram prawnych określających przekazywanie i przetwarzanie danych PNR.

Zakres stosowania dyrektywy jest ograniczony, ponieważ: przewiduje ona zatrzymanie danych PNR w JIP przez okres nieprzekraczający pięciu lat, po upływie którego dane powinny zostać usunięte; przewiduje poddanie danych depersonalizacji poprzez maskowanie elementów danych po upływie początkowego okresu sześciu miesięcy oraz zakazuje zbierania i wykorzystywania danych szczególnie chronionych. W celu zapewnienia skuteczności i wysokiego poziomu ochrony danych państwa członkowskie są zobowiązane do zapewnienia, by za doradztwo i monitorowanie w zakresie sposobu przetwarzania danych PNR odpowiadał niezależny krajowy organ nadzorczy oraz, w szczególności, inspektor ochrony danych. Wszelkie operacje przetwarzania danych PNR powinny być ewidencjonowane lub dokumentowane na potrzeby weryfikacji zgodności z prawem tych operacji, monitorowania własnej działalności oraz zapewnienia odpowiedniej integralności danych i bezpiecznego przetwarzania. Ponadto państwa członkowskie powinny zapewnić, by pasażerowie byli informowani w sposób jasny i dokładny o zbieraniu danych PNR i o przysługujących im prawach.

Zgodnie z art. 3 Protokołu nr 21 w sprawie stanowiska Zjednoczonego Królestwa i Irlandii w odniesieniu do przestrzeni wolności, bezpieczeństwa i sprawiedliwości, załączonego do Traktatu o Unii Europejskiej i Traktatu o funkcjonowaniu Unii Europejskiej, te dwa państwa członkowskie powiadomiły o chęci uczestniczenia w przyjęciu i stosowaniu dyrektywy.

Zgodnie z art. 1 i 2 Protokołu nr 22 w sprawie stanowiska Danii, załączonego do Traktatu o Unii Europejskiej i do Traktatu o funkcjonowaniu Unii Europejskiej, Dania nie uczestniczy w przyjęciu dyrektywy i nie jest nią związana ani jej nie stosuje.

Podsumowując, należy podkreślić, że wiele organizacji pozarządowych zgłaszało uwagi do projektu dyrektywy. Organizacje stawiały pytanie co stało się z koniecznością zapewnienia

równowagi pomiędzy wymogami związanymi z zapewnieniem bezpieczeństwa, a gwarancjami w zakresie praw podstawowych. Wysuwano zastrzeżenia co do pozyskiwania danych o pasażerach przez służby. Organy państwa na podstawie dyrektywy uzyskają nieograniczony dostęp do szczegółowych danych pasażera. Dane te można podzielić na dwie grupy. Pierwsza, są to dane osobowe pasażera w zakresie imienia, nazwiska, wieku itd. Druga grupa dotyczy natomiast danych o locie. Pasażer zobowiązany jest do podania szczegółowych informacji (m.in. dane kontaktowe osoby dokonującej rezerwacji, adnotacje o niestawieniu się na lot czy kontakt do agencji turystycznej lub biura linii lotniczych, w których dokonano rezerwacji). Celem dyrektywy jest zapobieganie i zwalczanie przestępstw terrorystycznych oraz innych poważnych przestępstw, ale cel ten może zmierzać również ku profilowaniu i ograniczaniu prywatności. Profilowanie sprowadza się do sklasyfikowania podróżnego pod kątem takich kryteriów, jak pochodzenie etniczne, miejsce do którego leci czy informacje o powrocie. Może również być źródłem danych marketingowych.

Kolejne wątpliwości dotyczą kwestii powołania urzędników ds. ochrony danych w każdej jednostce ds. informacji o pasażerach. Jakie warunki powinien spełnić kandydat na takie stanowisko i jakie będzie posiadał kompetencje powinny zostać szczegółowo określone. Należy także wzmocnić uprawnienia organów ochrony danych w zakresie monitorowania wykorzystywanych danych PNR, a także rygorystyczne warunki dostępu do zanonimizowanych danych PNR po upływie sześciu miesięcy. Kto będzie mógł mieć do nich dostęp, w jakich sytuacjach i na jakiej podstawie prawnej.

Należy zauważyć, że przyjęcie dyrektywy PNR pozwoli na zwalczanie najpoważniejszych zagrożeń dla bezpieczeństwa obywateli z odpowiednim wyprzedzeniem. Aktywność służb będzie bazowała przede wszystkim na informacjach przekazanych przez jednostki ds. informacji na dwa sposoby. Pierwszą z nich jest metoda „pobierania" polegająca na tym, że właściwe organy państw członkowskich potrzebujące danych mogą sięgnąć (skorzystać z dostępu) do systemu rezerwacji przewoźnika lotniczego i uzyskać kopię potrzebnych danych. Druga zaś to metoda „dostarczania", polegająca na tym, że przewoźnicy lotniczy i podmioty gospodarcze niebędące przewoźnikami przekazują potrzebne dane PNR na wniosek danego organu, co pozwala przewoźnikom lotniczym zachować kontrolę nad tym, jakie dane są przekazywane. Tym samym druga z metod zapewnia wyższy stopień ochrony danych osobowych.

PNR obejmuje m.in. imię i nazwisko pasażera, jego adres i numer telefonu, trasę lotu, numer miejsca w samolocie, informację o bagażu, środku płatniczym (np. numer karty kredytowej), czy też biurze turystycznym, z którego usług skorzystano. To także dane wrażliwe, związane m.in. z wyborem posiłku (np. halal czy dań koszernych), który może wynikać z wyznawanej religii, czy też informacje o zdrowiu pasażera (np. gdy pasażer zgłosi, że potrzebuje opieki na lotnisku lub w samolocie) oraz wspólnego lotu czy pokoju w hotelu. Wnioski wyciągane z tego typu informacji mogą prowadzić do stygmatyzacji oraz dyskryminacji konkretnych grup.

Nowa dyrektywa wyraźnie wskazuje, że dane mogą być zbierane, przechowywane i przetwarzane jedynie w celach zapobiegania i wykrywania poważnych przestępstw i aktów terrorystycznych. Niektórzy zwracają jednak uwagę, że trudno będzie zapewnić, że

wszystkie kraje UE będą ściśle trzymać się tych procedur. Jako przykład, co prawda spoza UE, podaje się „wyciek" poufnych danych-depesz dyplomatycznych przesyłanych między Departamentem Stanu USA, a ambasadami USA i publikację przez portal internetowy WikiLeaks w listopadzie 2010 roku.7 Z inicjatywy Parlamentu Europejskiego przewidziano, że po dwóch latach od wprowadzenia dyrektywy przez kraje UE dokonany będzie przegląd jej działania, aby skontrolować, czy przestrzegane są standardy dotyczące ochrony prywatności oraz czy dane wykorzystywane są w sposób proporcjonalny i zgodnie z celami dyrektywy. Od momentu opublikowania dyrektywy w Dzienniku Urzędowym Unii Europejskiej, państwa członkowskie mają dwa lata na wdrożenie jej zapisów do prawa krajowego.

Dyrektywa ma zastosowanie do "lotów poza UE", ale państwa członkowskie mogą również zdecydować o stosowaniu jej do lotów wewnątrzunijnych (czyli z kraju UE do jednego lub wielu krajów UE), pod warunkiem, że powiadomi o tym Komisję Europejską. Państwa członkowskie mogą również zdecydować się na zbieranie i przetwarzanie danych PNR przekazywanych przez biura podróży i organizatorów wycieczek świadczący usługi takie jak rezerwacja lotów.

Bibliography

Decyzja Rady z 6 czerwca 2003 roku dotycząca podpisania Umów między Unią Europejską a Stanami Zjednoczonymi Ameryki w sprawie ekstradycji oraz wzajemnej pomocy prawnej w sprawach karnych (2003/516/WE), Dz. U. L 181, 19.07.2003.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 roku w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, http://eur-lex.europa.eu/ LexUriServ/LexUriServ.do?uri=DD: 13:15: 31995L0046:PL:PDF (12.10. 2010).

Dyrektywa Rady 2004/82/WE z 29 sierpnia 2004 roku w sprawie zobowiązania przewoźników do przekazywania danych pasażerów.

Dyrektywa 95/46/WE Parlamentu Europejskiego i Rady z 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych, http://eur-lex.europa.eu/LexUriServ/do?uri=DD:13:15:31995L0046:PL:PDF (12.10. 2010).

Komunikat Komisji w sprawie globalnego podejścia do przekazywania danych dotyczących przelotu pasażera (PNR) państwom trzecim, KOM(2010) 492 wersja ostateczna, Bruksela, 21.09.2010, http://www.ulc.gov.pl/index.php? option=com_content&task=view&id=1180 (18.12. 2010).

Opinia nr 9/2006 dotycząca wdrożenia dyrektywy 2004/82/WE Rady w sprawie zobowiązania przewoźników do przekazywania z wyprzedzeniem danych pasażerów przyjęta 28 września 2006 r., http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2006/wp127_pl.pdf (18.10.2010).

Porozumienie 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, http://eur-lex.europa.eu/LexUriServ/LexUriServ. do?uri=OJ:L:2004: 183: 0083:0083:PL:PDF (12.6.2010).

Dr inż. pil. Tomasz Balcerzak-Ekspert Rady Naukowo-Technicznej Rządu Malty, Ekspert Europejskiej Agencji Nawigacji Satelitarnej, Wykładowca Politechniki Śląskiej, Katedry Technologii Lotniczych, 2013-2016r. Prezes Zarządu Polskiego Klubu Lotniczego, poprzednio Prezes Zarządu/Dyrektor Generalny Eurolot S.A. Od lipca 2011 do końca grudnia 2014 r. Przewodniczący Rady Nadzorczej spółki WRO LOT-usługi lotniskowe. Od maja 20011 do grudnia 2013 r. pełnił funkcję Członka Zarządu ds. Operacyjno-Technicznych w Polskich Liniach Lotniczych LOT m.in. koordynując szereg projektów w obszarze operacyjno-technicznym oraz nadzorując program restrukturyzacyjny. Od 2009 roku Tomasz Balcerzak pracował początkowo jako Prezes, a następnie Członek Zarządu oraz Dyrektor Operacyjny w czarterowej linii lotniczej Enter Air. Doświadczenie zawodowe zdobywał m.in. jako Pilot-Dowódca Załogi w 36. Specjalnym Pułku Lotnictwa Transportowego w Warszawie, Dyrektor Operacyjny w linii lotniczej Centralwings, a także Dyrektor Zarządzający w spółce FDS-Flight Dispatch Services oraz Dyrektor Jakości w linii lotniczej Fly Jet. Ukończył Wyższą Szkołę Oficerską Sił Powietrznych w Dęblinie otrzymując tytuł podporucznika pilota inżyniera. Wiedzę uzupełniał również podczas dodatkowych studiów magisterskich, następnie otrzymując tytuł doktora na Uniwersytecie Warszawskim oraz podczas studiów podyplomowych w Szkole Głównej Handlowej. Jest również wykładowcą m.in. prawa lotniczego oraz gospodarczych zagadnień transportu lotniczego i kosmicznego Instytutu Stosunków Międzynarodowych Uniwersytetu Warszawskiego oraz Uczelni Łazarskiego.

Ma bogate doświadczenie w branży lotniczej oraz w prowadzeniu projektów z obszaru operacyjnego firm. Jest założycielem i współzałożycielem kilku istniejących w Polsce przedsiębiorstw branży lotniczej. Specjalizuje się w zagadnieniach transportu, logistyki oraz prawa lotniczego i kosmicznego.

References

1. dr inż. Tomasz Balcerzak-Katedra Technologii Lotniczych, Wydziału Transportu Politechniki Śląskiej: tomasz.balcerzak@polsl.pl.

2. Traktat lizboński (Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską; w wersji roboczej określany jako traktat reformujący) – umowa międzynarodowa zakładająca m.in. reformę instytucji Unii Europejskiej, podpisana 13 grudnia 2007 roku w Lizbonie. Traktat wszedł w życie 1 grudnia 2009, przy czym w hierarchii źródeł prawa porządku prawnego Rzeczypospolitej Polskiej obowiązuje od chwili ogłoszenia w Dzienniku Ustaw, co nastąpiło 2 grudnia 2009 (Dz. U. z 2009 r. Nr 203, poz. 1569). Najważniejsze uzgodnienia zawarte w traktacie to: zmniejszenie liczby komisarzy europejskich do 18 (mimo że jest 28 państw członkowskich), zwiększenie liczby eurodeputowanych dla Włoch, decyzje unijne od 2014 będą podejmowane za pomocą tzw.

podwójnej większości, zamiast zgody wszystkich państw członkowskich, od 2009 Parlament Europejski będzie miał maksymalnie 750 członków (poprzednio 785), pośrednia inicjatywa ustawodawcza obywateli wymagać będzie zebrania 1 miliona głosów w danej sprawie, niewygasalność tzw. „kompromisu z Janiny", przyznanie Polsce dodatkowego Europosła, wprowadzenie stanowiska wysokiego przedstawiciela Unii ds. zagranicznych i polityki bezpieczeństwa, wprowadzenie stanowiska Przewodniczącego Rady Europejskiej, Karta praw podstawowych, „solidarność energetyczna".

3. W dniach 10-11 grudnia 2009 r. Rada Europejska przyjęła nowy program rozwoju przestrzeni wolności, bezpieczeństwa i sprawiedliwości (PWBiS) Unii Europejskiej. Dokument zatytułowany „Program Sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli" – plan wspólnego działania rządów krajów Unii Europejskiej w ramach rozwoju III filaru UE – współpracy sądowej i policyjnej w sprawach karnych. Przyjęty został na spotkaniu Rady Europejskiej w Tampere.

4. Interfejs programistyczny aplikacji (ang. Application Programming Interface, API) – sposób, rozumiany jako ściśle określony zestaw reguł i ich opisów, w jaki programy komputerowe komunikują się między sobą. API definiuje się na poziomie kodu źródłowego dla takich składników oprogramowania jak np. aplikacje, biblioteki czy system operacyjny. Zadaniem API jest dostarczenie odpowiednich specyfikacji podprogramów, struktur danych, klas obiektów i wymaganych protokołów komunikacyjnych.

5. Dane dotyczące przelotu pasażera zbierane przez przewoźników lotniczych: 1. Kod identyfikacyjny danych PNR; 2. Data rezerwacji/wystawienia biletu; 3. Data(-y) planowanej podróży; 4. Imię i nazwisko (imiona i nazwiska); 5. Adres i dane kontaktowe (numer telefonu, adres e-mail); 6. Wszystkie informacje o formie płatności, w tym adres na fakturze; 7. Kompletna trasa podróży dla konkretnych danych PNR; 8. Informacje o programach lojalnościowych; 9. Biuro podróży/agencja turystyczna; 10. Dane o statusie podróży pasażera, w tym potwierdzenia, stan odprawy biletowo-bagażowej, dane typu: pasażer nie stawił się lub pasażer nabył bilet w czasie odprawy bez wcześniejszej rezerwacji; 11. Informacje o podzieleniu/rozdzieleniu danych PNR; 12. 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); 13. Informacje o wystawieniu biletu, w tym numer biletu, data wystawienia biletu i bilety w jedną stronę, informacja o automatycznie skalkulowanej taryfie; 14. Numer miejsca na pokładzie i inne informacje o miejscu; 15. Informacje o wspólnej obsłudze połączeń; 16. Wszystkie informacje o bagażu; 17. Liczba oraz imiona i nazwiska innych podróżnych wymienionych w PNR; 18. Wszelkie zebrane dane pasażera przekazane przed podróżą (dane API) (w tym rodzaj, numer, kraj wydania i data ważności dokumentu tożsamości, obywatelstwo, nazwisko, imię, płeć, data urodzenia, linia lotnicza, numer lotu, data odlotu, data przylotu, port lotniczy odlotu, port lotniczy przylotu, godzina odlotu i godzina przylotu); 19. Wszystkie dotychczasowe zmiany danych PNR wymienionych w pkt 1–18.

6. Załącznik II-Wykaz przestępstw, o których mowa w art. 3 pkt 9: 1. Udział w organizacji przestępczej; 2. Handel ludźmi; 3. Wykorzystywanie seksualne dzieci i pornografia dziecięca; 4. Nielegalny handel narkotykami i substancjami psychotropowymi; 5. Nielegalny handel bronią, amunicją i materiałami wybuchowymi; 6. Korupcja; 7. Oszustwo, w tym oszustwo przeciwko interesom finansowym Unii; 8. Pranie dochodów z przestępstwa i fałszowanie pieniędzy, w tym euro; 9. Przestępczość komputerowa i cyberprzestępczość; 10. Przestępstwa przeciwko środowisku, w tym nielegalny handel zagrożonymi gatunkami zwierząt oraz zagrożonymi gatunkami i odmianami roślin; 11. Ułatwianie bezprawnego wjazdu i pobytu; 12. Zabójstwo, spowodowanie ciężkiego uszczerbku na zdrowiu; 13. Nielegalny obrót organami i tkankami ludzkimi; 14. Uprowadzenie, bezprawne pozbawienie wolności i wzięcie zakładników; 15. Kradzież zorganizowana i rozbój przy użyciu broni; 16. Nielegalny handel dobrami kultury, w tym antykami i dziełami sztuki, 17. Podrabianie i piractwo produktów; 18. Fałszowanie dokumentów urzędowych i handel nimi; 19. Nielegalny handel substancjami hormonalnymi i innymi środkami pobudzającymi wzrost; 20. Nielegalny handel materiałami jądrowymi lub promieniotwórczymi; 21. Zgwałcenie; 22. Przestępstwa podlegające jurysdykcji Międzynarodowego Trybunału Karnego; 23. Bezprawne zawładnięcie statkiem powietrznym lub statkiem; 24. Sabotaż; 25. Handel skradzionymi pojazdami; 26. Szpiegostwo przemysłowe.

7. Należy podkreślić, iż ten bezprecedensowy „przeciek" z 28 listopada 2010 roku objął 200 z 251 287 dokumentów. Spośród dokumentów żaden nie jest oznaczony klauzulą „ściśle tajne", ok. 15 tys. to dokumenty „tajne", ok. 100 tys. „poufne" a 130 tys. nie zostało sklasyfikowanych. Szerzej: Secret US Embassy Cables, http://213.251.145.96/cablegate.html (18.12.2010).