FUNDACJA PANOPTYKON

PRISM, SWIFT, PNR, Safe Harbour, czyli jak Amerykanie próbują zrozumieć świat

„Powinniśmy zakładać, że każda służba wywiadu, nie tylko nasza, ale każda europejska służba wywiadu, każda azjatycka służba wywiadu (...) będzie dążyć do tego, by spróbować zrozumieć świat oraz co się dzieje w światowych stolicach".

Tymi słowami Barack Obama skomentował medialne doniesienia o tym, że Narodowa Agencja Bezpieczeństwa (National Security Agency, NSA) mogła podsłuchiwać rozmowy unijnych urzędników oraz szpiegowała wewnętrzną sieć komputerów Unii Europejskiej. Informacje o tym oraz o programie PRISM ujawnione przez Edwarda Snowdena wzburzyły europejską opinię publiczną. Komisarz ds. sprawiedliwości i praw podstawowych Unii Europejskiej, Viviane Reding, zadała Prokuratorowi Generalnemu USA siedem pytań drążących zasady dostępu NSA i FBI do danych klientów amerykańskich firm, które miały uczestniczyć w programie PRISM. Do tej pory nie uzyskała odpowiedzi.

PRISM i inne działania NSA to tylko skrajny przykład konsekwentnej strategii gromadzenia danych o obywatelach innych państw na potrzeby bezpieczeństwa wewnętrznego, którą Stany Zjednoczone realizują od ponad 10 lat. Na tę strategię składają się nie tylko tajne programy, ale przede wszystkim jawne porozumienia międzynarodowe o przekazywaniu danych w różnych celach związanych z bezpieczeństwem i amerykańskie prawo, które na firmy objęte jurysdykcją USA nakłada obowiązek współpracy z wywiadem i służbami specjalnymi. Poniżej wyjaśniamy, jakimi drogami dane obywateli Unii Europejskiej trafiają do Stanów Zjednoczonych i jakie konsekwencje ma to dla ochrony prywatności. Przedstawiamy najważniejsze fakty, podstawy prawne, kontrowersje i opinie różnych środowisk.

Celem tego opracowania jest wzbogacenie wywołanej przez Edwarda Snowdena debaty o informacje o jawnych, choć niekoniecznie powszechnie znanych, sposobach pozyskiwania danych Europejczyków. Jednocześnie chcemy pokazać, że krytykowane dziś praktyki wywiadu USA nie są niczym nowym (co nie znaczy, że dopuszczalnym), a grunt dla ich realizacji – w postaci ogromnych zasobów danych obywateli Unii Europejskiej w rękach amerykańskich firm i instytucji – został stworzony przy wiedzy i współpracy instytucji europejskich.

Fundacja Panoptykon

Warszawa, 10 lipca 2013 r.

DROGA PIERWSZA: LINIE LOTNICZE

Dane pasażerów linii lotniczych przekazywane na podstawie porozumienia w sprawie PNR

Od kilku lat dane pasażerów linii lotniczych (Passenger Name Records, PNR) są wykorzystywane przez organy ścigania, głównie amerykańskie, na potrzeby walki z terroryzmem i poważną przestępczością. Dane PNR wszystkich pasażerów samolotów lecących z Europy do USA trafiają do Departamentu Bezpieczeństwa Wewnętrznego (Departament of Home Security, DHS) jeszcze zanim samolot wystartuje. Na tej podstawie DHS weryfikuje, czy wśród pasażerów znajdują się osoby mogące stanowić zagrożenie dla bezpieczeństwa USA. DHS prowadzi czarną listę osób podejrzanych o popełnienie przestępstwa lub terroryzm (tzw. *no fly list*).

Czym dokładnie są dane PNR?

PNR to dane o pasażerach, zbierane zwyczajowo przez linie lotnicze w celach komercyjnych. 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 bardzo wrażliwie informacje**, takie jak preferencje dotyczące posiłku serwowanego na pokładzie samolotu (koszerny, wegetariański czy bez wieprzowiny) albo fakt rezerwowania pokoju z podwójnym łóżkiem.

Kogo dotyczy przekazywanie danych?

Pasażerów wszystkich samolotów lecących do Stanów Zjednoczonych.

Kto i jak je przetwarza?

W większości dane PNR są przetwarzane przez firmy obsługujące systemy rezerwacyjne zwane Computerized Reservation Systems (CRS). W każdym CRS znajdują się kopie danych PNR ze wszystkich lotów wszystkich linii lotniczych oraz agencji turystycznych, które obsługuje. Z czterech głównych systemów CRS aż trzy są własnością firm amerykańskich.

Na jakiej podstawie dochodzi do przekazywania danych?

Podstawą prawną przekazywania danych jest umowa między USA a Unią Europejską o wykorzystywaniu i przekazywaniu danych pasażerów linii lotniczych (tzw. **porozumienie PNR**). Unia Europejska jest związana porozumieniem PNR od 2004 r. Pierwsza wersja porozumienia na fali krytyki ze strony Parlamentu Europejskiego została poddana rewizji, jako niespełniająca standardów zawartych w europejskiej dyrektywie o ochronie danych osobowych. Kolejna, zrewidowana wersja weszła w życie 1 lipca 2012 r. [1].

Jakie budzi kontrowersje?

1) Nie ma dowodów na to, że przekazywanie danych pasażerów linii lotniczych pozwala zmniejszyć zagrożenie atakami terrorystycznymi, natomiast w istotny sposób ogranicza prywatność pasażerów i stwarza ryzyko poważnych nadużyć.
2) W praktyce wykorzystywanie danych PNR oznacza automatyczne profilowanie każdego podróżnego, jako potencjalnie podejrzanego o terroryzm. Na podstawie ograniczonych danych z systemów rezerwacyjnych wyciągane są kontrowersyjne wnioski, a na czarną listę 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).
3) Porozumienie PNR nie przewiduje realnych gwarancji ochrony praw obywateli UE w USA. 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 odpowiednich gwarancji ochrony danych osobowych: udostępniane są niezabezpieczone kopie danych, a tzw. lokalizator rejestru pozwala sprawdzającemu odtworzyć komplet danych osobowych przechowywanych w systemie rezerwacyjnym. Wreszcie, w przypadku umieszczenia na czarnej liście obywatel UE nie może skorzystać z żadnej procedury odwoławczej.
4) Dane pasażerów lecących z Europy są przechowywane w USA przez 15 lat. To wielokrotnie dłużej niż np. dane telekomunikacyjne przechowywane przez operatorów na potrzeby walki z poważną przestępczością. Dla porównania, dane pasażerów lecących do USA z Kanady są przechowywane przez 5,5 roku, a z Australii – 3,5 roku.
5) Gwarancje dotyczące maksymalnego czasu przechowywania danych i obowiązku ich usunięcia po upływie tego czasu są pozorne i nieegzekwowalne w praktyce.
6) Nie wiadomo, do jakich jeszcze celów (poza zwalczaniem terroryzmu i poważnej przestępczości) mogą zostać wykorzystane dane PNR. Samo porozumienie przewiduje ich wykorzystywanie także w przypadku postępowań sądowych oraz bliżej nieokreślonych „spraw związanych z przekraczaniem granicy".

[1] Treść porozumienia PNR, http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do?step=0&redirect=true&treatyId=9382, [dostęp: 8.07.2013].

DROGA DRUGA: SYSTEM BANKOWY

Dane o transakcjach finansowych przekazywane na podstawie porozumienia SWIFT

Po atakach z 11 września 2001 r. Stany Zjednoczone zażądały od stowarzyszenia instytucji finansowych SWIFT udostępniania na potrzeby walki z terroryzmem danych o transakcjach bankowych. Program ma pomóc w śledzeniu źródeł finansowania działalności terrorystycznej. Od 2010 r. banki i instytucje finansowe zarejestrowane w Unii Europejskiej są zobowiązane do przekazywania amerykańskim służbom hurtowych ilości danych osobowych swoich klientów. Przekazywanie danych jest realizowane za pośrednictwem sieci SWIFT.

Czym jest SWIFT?

Society for Worldwide Interbank Financial Telecommunication (SWIFT) to stowarzyszenie instytucji finansowych utrzymujące sieć telekomunikacyjną służącą do wymiany informacji. SWIFT pośredniczy w transakcjach między bankami, domami maklerskimi, giełdami oraz innymi instytucjami finansowymi. Dziennie realizowanych jest kilka milionów operacji. W większości z nich uczestniczą kraje europejskie. SWIFT odpowiada za 80 % przelewów elektronicznych w 208 krajach.

Kogo dotyczy przekazywanie danych?

Wszystkich klientów banków i instytucji finansowych zarejestrowanych w Unii Europejskiej.

Na jakiej podstawie dochodzi do przekazywania danych?

Podstawą prawną dla przekazywania danych o transakcjach finansowych jest tzw. **porozumienie SWIFT**: umowa między Unią Europejską a USA o przetwarzaniu i przekazywaniu danych z komunikatów finansowych w celu śledzenia środków finansowych należących do terrorystów z 2010 r.

Jakie budzi kontrowersje?

1) Porozumienie SWIFT to rażący przykład braku transparentności, a sposób jego realizacji prowadzi do systemowych naruszeń europejskich standardów ochrony danych osobowych. Do takich wniosków doszła międzynarodowa grupa ekspertów odpowiedzialna za ocenę realizacji porozumienia SWIFT w 2011 r.[2].
2) Hurtowe przekazywanie danych narusza obowiązujące w europejskim prawie zasady niezbędności i proporcjonalności.
3) Teoretycznie, by uzyskać dostęp do danych bankowych osób podejrzanych o terroryzm lub wspieranie terroryzmu, służby amerykańskie potrzebują zgody Europolu. W praktyce dostęp do tych danych nie wymaga ani wykazania, że dana osoba znajduje się w kręgu podejrzeń, ani że toczy się w jej sprawie jakiekolwiek postępowanie.
4) Zapytania amerykańskich służb nie zawierają ani jasnego określenia zakresu pobieranych danych, ani celu, w jakim są pobierane. Zdaniem ekspertów oceniających realizację porozumienia SWIFT, ma to szczególne znaczenie, „gdy w grę wchodzą tak duże ilości informacji, również o osobach, które nie są podejrzane o działalność terrorystyczną"[3].
5) Obywatele UE, nawet jeśli dowiedzą się, że ich dane zostały bezprawnie przekazane przez system SWIFT, nie mogą dochodzić roszczeń – prawo USA nie daje takiej możliwości osobom nie będącym obywatelami USA.

Opinie na temat porozumienia SWIFT:

> *Ten raport powinien stanowić sygnał alarmowy dla Brukseli. Prawdopodobnie Europol nie przestrzega gwarancji ochrony danych osobowych, na które nalegaliśmy, i które były jednym z warunków zawarcia porozumienia. Musimy wyjaśnić, jak te transfery się odbywają. Wydaje się, że Europol autoryzuje spore transfery danych na podstawie nieakceptowalnych, szerokich zapytań ze strony USA oraz nigdzie niezapisanych, ustnie przekazywanych informacji*[4].
>
> — **Sophie in't Veld**, holenderska eurodeputowana reprezentująca Parlament Europejski w pracach nad porozumieniem SWIFT, o raporcie Europolu.

> *Podstawowe problemy związane z tym porozumieniem pozostają nierozwiązane: wciąż nie wiadomo, jaki zakres i do jakiego stopnia dane są przekazywane do USA*[5].
>
> — **Peter Schaar**, Niemiecki Federalny Komisarz Ochrony Danych.

---

[2] ALDE, Terrorist Finance Tracking Programme is not respecting data protection safeguards, http://www.alde.eu/fr/presse/communiques-presse-et-nouvelles/communiques-de-presse/article/terrorist-finance-tracking-programme-is-not-respecting-data-protection-safeguards-37202/, [dostęp: 8.07.2013].

[3] Europol Review, General Report on Europol Activities https://www.europol.europa.eu/sites/default/files/publications/europolreview2011.pdf, [dostęp: 10.07.2013].

[4] ALDE, ibid.

[5] EDRi, Is the Commission's report on Swift agreement biased?, http://www.edri.org/edrigram/number11.1/ec-swift-agreement-report, [dostęp: 8.07.2013].

DROGA TRZECIA: SERWERY AMERYKAŃSKICH FIRM

Transfery danych między spółkami w ramach programu „Bezpieczna Przystań"

Od 2000 r. amerykańskie firmy, które działają na europejskim rynku i chciałyby przekazywać dane swoich klientów do USA, mogą to robić w ramach programu *Safe Harbour* („Bezpieczna Przystań"). Mimo że europejskie prawo o ochronie danych osobowych co do zasady zakazuje przekazywania danych do państw niezapewniających odpowiedniego standardu w tym zakresie, amerykańskim firmom, które przystąpią do programu, wystarcza certyfikat gwarancji przestrzegania przepisów dyrektywy 95/46/WE o ochronie danych osobowych. To bardzo słaba, bo jedynie papierowa, gwarancja ochrony danych obywateli UE przed ich nadużywaniem w celach komercyjnych, nie wspominając o wykorzystywaniu przez wywiad czy służby specjalne. W programie *Safe Harbour* uczestniczy ok. 1100 amerykańskich firm.

Kogo dotyczy przekazywanie danych?

Klientów firm, których siedziba jest zarejestrowana w USA oraz firm, które działają na rynku europejskim, ale z różnych powodów przekazują posiadane przez siebie dane do USA.

Na jakiej podstawie dochodzi do przekazywania danych?

Program *Safe Harbour* został zatwierdzony przez Unię Europejską decyzją Komisji 2000/520/WE z dnia 26 lipca 2000 r. Mimo braku odpowiednich gwarancji ochrony danych osobowych w prawie USA, Komisja uznała, że sam program daje takie gwarancje.

Jakie gwarancje ochrony praw obywateli UE przewiduje program *Safe Harbour*?

Teoretycznie obywatele UE mogą składać skargi do narodowych rzeczników ochrony danych osobowych, które następnie są przekazywane organom amerykańskim. Jednak nadzór amerykańskiej Federal Trade Commission nad firmami uczestniczącymi w programie *Safe Harbour* jest częściowy (nie obejmuje niektórych sektorów, w których może dochodzić do przetwarzania danych) i ma charakter formalny. Same transfery danych nie wymagają zgody ani powiadomienia żadnego organu. Tylko w przypadku, gdy dana firma **nie** jest członkiem programu *Safe Harbour*, do przekazania danych do USA wymagana jest zgoda odpowiedniego organu ochrony danych osobowych (w Polsce – GIODO).

Jakie budzi kontrowersje?

1) Program *Safe Harbour* przewiduje bardzo łagodne warunki przystąpienia dla amerykańskich firm i pozostawia im szerokie pole do interpretacji.
2) Zasadniczo program zakłada, że firmy same na siebie będą nakładać obowiązki w zakresie ochrony danych osobowych.
3) W USA brakuje efektywnych mechanizmów egzekwowania ustaleń wynikających z programu *Safe Harbour*: do tej pory Federal Trade Commission tylko raz wszczęła procedurę egzekwowania zasad programu wobec jednego z sygnatariuszy. Analizując prawo USA, w 2010 r. grupa niemieckich rzeczników ochrony danych osobowych w ogóle zakwestionowała możliwości egzekwowania zasad programu *Safe Harbour* przez organy amerykańskie[6].
4) Grupa Robocza Art. 29, zrzeszająca europejskich rzeczników ochrony danych osobowych, uznała, że program nie zapewnia odpowiedniego poziomu ochrony danych osobowych. W przedstawionej przez nią opinii czytamy, że Grupa „wciąż jest zaniepokojona liczbą problemów, w stosunku do których możliwe byłoby zapewnienie lepszego standardu ochrony danych osobowych".
5) Dostęp amerykańskich służb i organów egzekwowania prawa do danych przetwarzanych przez amerykańskie firmy: od momentu, gdy na podstawie programu *Safe Harbour* dane obywateli UE zostaną przekazane amerykańskim firmom, zaczyna działać prawo USA, m.in. FISAA (patrz niżej). Na tej podstawie amerykańskie służby i organy egzekwowania prawa zyskują dostęp do naszych danych z całkowitym pominięciem standardów wyznaczonych przez przepisy prawa UE.

Opinie na temat ogólnych relacji UE – USA w obszarze transferu danych

> *Stany Zjednoczone nie są krajem bezpiecznym, jeśli chodzi o przetwarzanie danych osobowych*[7].
>
> — **Wojciech Wiewiórowski**, Generalny Inspektor Ochrony Danych Osobowych

> *Skoro sama Unia Europejska nie dąży konsekwentnie do zwiększenia wagi praw podstawowych, w tym ochrony danych osobowych, trudno tego oczekiwać od reszty świata*[8].
>
> — **Peter Hustinx**, Europejski Rzecznik Ochrony Danych Osobowych

[6] Chris Connolly, The US Safe Harbor - Fact or Fiction?, http://www.galexia.com/public/research/articles/research_articles-pa08.html, [dostęp: 10.07.2013].
[7] Antyweb, GIODO o aferze PRISM – dlaczego USA są niebezpieczne,http://antyweb.pl/giodo-o-aferze-prism-dlaczego-usa-sa-niebezpieczne-wywiad/ [dostęp: 8.07.2013].
[8] Statewatch, http://www.statewatch.org/news/2007/jun/eu-us-pnr-hustinx-letter.pdf, [dostęp: 8.07.2013].

POST SCRIPTUM: RAMY PRAWNE AMERYKAŃSKIEGO SYSTEMU NADZORU

Foreign Intelligence Surveillance Act

PRISM i inne programy nadzorcze realizowane przez amerykańskie służby, w szczególności FBI i NSA, nie są zawieszone w prawnej próżni. Powyżej staraliśmy się pokazać, w jaki sposób dane obywateli Unii Europejskiej trafiają na terytorium USA lub serwery amerykańskich firm i wyjaśnić, że nie dzieje się to bez przyzwolenia i wiedzy instytucji europejskich. O realnych możliwościach wykorzystywania danych Europejczyków przez amerykańskie służby nie przesądza jednak prawo unijne, ale prawo USA, na które jako obcokrajowcy nie mamy żadnego wpływu. Podstawowym dokumentem, na podstawie którego w świetle prawa mogą funkcjonować programy takie jak PRISM, jest Foreign Intelligence Surveillanc Act (FISA).

Co to jest FISA?

Foreign Intelligence Surveillance Act to akt prawny przyjęty przez amerykański Kongres w 1978 r. w odpowiedzi na nieprawidłowości, jakich dopuszczały się amerykańskie służby wywiadowcze. Ustawa, określająca zasady działania amerykańskich służb w odniesieniu do cudzoziemców, była wielokrotnie nowelizowana. Do najistotniejszej nowelizacji doszło w 2008 r., czyli już za kadencji prezydenta Obamy, kiedy dopisano do niej sekcję 1881a. Od tego momentu FISA bywa określana jako Foreign Intelligence Surveillance Amendment Act (FISAA)[9].

Jakie możliwości FISA daje amerykańskim służbom i w kogo jest wymierzona?

Sekcja 1881a odwraca pierwotną logikę tego aktu prawnego, dając amerykańskim służbom w zasadzie nieograniczone prawo inwigilowania „osób, co do których można racjonalnie przypuszczać, że znajdują się poza Stanami Zjednoczonymi"[10]. Te osoby mogą być w świetle prawa namierzane (*targeted*) w celu pozyskania „zagranicznej informacji wywiadowczej"[11]. Nie ulega wątpliwości, że sekcja 1881a została napisana z myślą o obcokrajowcach. Nie dotyczy ona obywateli i rezydentów USA, nawet jeśli przez dłuższy czas pozostają poza granicami kraju.

Zgodnie z FISA „zagraniczną informacją wywiadowczą" jest każda informacja, która może okazać się przydatna w związku z przeciwdziałaniem sabotażowi, terroryzmowi, działalności wywiadowczej obcych sił czy dla ochrony bezpieczeństwa narodowego USA, a także dla prowadzenia polityki zagranicznej. To bardzo szerokie kategorie, które pozwalają na gromadzenie informacji i monitorowanie m.in obcych rządów, polityków, organizacji społecznych. W grę może wchodzić pozyskiwanie wszelkich typów treści: dokumentów, komunikatów przesyłanych drogą elektroniczną, komunikatów głosowych, zdjęć.

Z jakich źródeł amerykańskie służby mogą pozyskiwać informacje?

Sekcja 1881a pozwala na gromadzenie informacji bezpośrednio od wszystkich operatorów telekomunikacyjnych i dostawców usług internetowych. W tej kategorii mieszczą się zarówno dostawcy usług telekomunikacyjnych (dostępu do Internetu, telefonii stacjonarnej i mobilnej), jak również firmy świadczące usługi oparte na przetwarzaniu danych w chmurze (np. hosting, poczta elektroniczna, portale społecznościowe, blogi etc.).

Jaka jest sytuacja prawna firm współpracujących ze służbami?

Dostawcy usług w zasadzie nie mają możliwości odrzucenia wniosków, które otrzymują od służb. Mogą to zrobić w bardzo ograniczonych przypadkach np. gdy wniosek dotyczy obywatela USA. Z drugiej strony firmy, które udzielają służbom informacji w oparciu o sekcję 1881a, nie mogą być z tego tytułu pociągnięte do odpowiedzialności.

Jakie procedury obowiązują amerykańskie służby?

Do pozyskania danych na podstawie sekcji 1881a FISA nie jest potrzebny nakaz sądowy. Rząd, działając za pośrednictwem Prokuratora Generalnego USA i Szefa Wywiadu (*Director of National Intelligence*), zwraca się do specjalnego, tajnego sądu – Foreign Intelligence Surveillance Court – z wnioskiem o „autoryzację" planowanej inwigilacji. Autoryzacja nie dotyczy konkretnej sprawy; jest przyznawana na okres do 12 miesięcy i może być przedłużona o kolejne lata. W swoim wniosku rząd bardzo ogólnie określa cele inwigilacji i zapewnia, że nie będzie ona wymierzona w obywateli USA. W pilnych sprawach może też działać, nie czekając na sąd.

Czy FISA przewiduje jakiekolwiek gwarancje chroniące obywateli innych państw przed nadużyciami?

Nie. Zgodnie z FISA możliwości, jakie daje sekcja 1881a powinny być wykorzystywane zgodnie z czwartą poprawką do Konstytucji USA, chroniącą przed „nieracjonalnym przeszukaniem lub kontrolą". Niestety, czwarta poprawka, zgodnie z orzeczeniem Sądu Najwyższego USA, nie chroni obywateli innych państw.

---

[9] Pełna treść aktu prawnego: http://thomas.loc.gov/cgi-bin/query/z?c110:H.R.6304:, [dostęp: 10.07.2013].
[10] W oryginale: „persons reasonably believed to be located outside the United States".
[11] W oryginale: „to acquire foreign intelligence information".