(Tłumaczenie)

Przetwarzanie przez Departament Skarbu USA — na użytek walki z terroryzmem — danych osobowych pochodzących z UE — „SWIFT"

(2007/C 166/09)

Program śledzenia środków finansowych należących do terrorystów — Wyjaśnienia Departamentu Skarbu Stanów Zjednoczonych

W poniższych wyjaśnieniach przedstawiono Program śledzenia środków finansowych należących do terrorystów (program TFTP), realizowany przez Departament Skarbu USA, a zwłaszcza ścisłe kontrole i zabezpieczenia, którym podlega traktowanie danych uzyskanych od SWIFT na mocy wezwań administracyjnych, wykorzystywanie tych danych i ich rozpowszechnianie. Kontrole i zabezpieczenia stosuje się do wszystkich osób mających dostęp do danych SWIFT, chyba że w konkretnych przypadkach wskazano inaczej — m.in. w przypadku udostępniania wskazówek zaczerpniętych z danych SWIFT zagranicznym rządom.

Omawiany program ma podstawy prawne, konkretnych adresatów, jest użyteczny i owocny i przewiduje zabezpieczenia dotyczące prywatności. Dokładnie odzwierciedla on oczekiwania i nadzieje, które obywatele wiążą z ochroną przed zagrożeniem terrorystycznym i których spełnienia spodziewają się od swoich rządów.

Program śledzenia środków finansowych należących do terrorystów, realizowany przez Departament Skarbu USA

Wkrótce po zamachach z 11 września 2001 r., kiedy to starano się zastosować wszelkie możliwe środki, by wyśledzić terrorystów i tworzone przez nich siatki, w Departamencie Skarbu zainicjowano tytułowy program. W ramach tego programu departament zwrócił się z wezwaniem administracyjnym do amerykańskiego centrum operacji należącego do Stowarzyszenia na rzecz Światowej Międzybankowej Telekomunikacji Finansowej (SWIFT), by udostępniło mu dane związane z terroryzmem; stowarzyszenie to — mające siedzibę w Belgii — obsługujące światowy system komunikacyjny wykorzystywany do przekazywania informacji o transakcjach finansowych. We wspomnianych wezwaniach zwrócono się do SWIFT o dostarczenie Departamentowi Skarbu pewnych zapisów transakcji finansowych — które to zapisy przechowuje się w amerykańskim centrum operacji SWIFT w toku zwykłych prac — wyłącznie na użytek walki z terroryzmem, tak jak to wyjaśniono w dalszych częściach dokumentu.

Podstawowe założenia programu TFTP

Program TFTP został stworzony i od samego początku był realizowany tak, by spełniał wszystkie stosowne amerykańskie wymogi prawne, by w istotny sposób przyczyniał się do walki ze światowym terroryzmem oraz by respektował i chronił informacje, które są zawarte w danych SWIFT przechowywanych w USA i które potencjalnie wymagają szczególnej ochrony ze względów prywatnych i handlowych. Program bierze pod uwagę potencjalny wymóg szczególnej ochrony — ze względów prywatnych lub handlowych — informacji, którymi się posługuje, a zabezpieczenia wyszczególnione w niniejszych wyjaśnieniach stosuje niezależnie od obywatelstwa czy miejsca zamieszkania konkretnej osoby. Program przewiduje wielorakie i wielokrotne kontrole ze strony rządu i podmiotów niezależnych; kontrole te mają zagwarantować, że dane — których ilość jest z natury ograniczona — będą przeszukiwane wyłącznie na użytek walki z terroryzmem oraz że wszystkie będą przechowywane w bezpiecznym miejscu i traktowane we właściwy sposób.

Wszelkie działania Departamentu Skarbu, które służą uzyskaniu konkretnych informacji z amerykańskiego centrum operacji SWIFT oraz wykorzystaniu tych informacji wyłącznie po to, by prowadzić dochodzenia w sprawie terroryzmu lub finansowania działań terrorystycznych, by wykrywać te zjawiska, zapobiegać im lub ścigać ich sprawców, albo po to, by prowadzić związane z tym dochodzenia i wnosić akty oskarżenia, są zgodne z prawem USA. Poza tym danych udostępnianych przez SWIFT nie przeszukuje się, by zgromadzić dowody lub wykryć działalność niezwiązaną z terroryzmem lub z finansowaniem działań terrorystycznych, nawet jeżeli taka działalność byłaby bezprawna. Departament Skarbu nie przeszukuje danych SWIFT ani nie może wykorzystywać pochodzących z nich informacji w związku z ogólnymi dochodzeniami w sprawie uchylania się od podatków, prania pieniędzy, szpiegostwa gospodarczego, handlu narkotykami czy innej działalności przestępczej — chyba że w pewnym momencie była ona powiązana z terroryzmem lub finansowaniem działań terrorystycznych.

Dane uzyskane od SWIFT na mocy wezwań składają się z kopii komunikatów o przeprowadzonych transakcjach finansowych, tj. z elektronicznych kopii zapisów o działalności gospodarczej przechowywanych w amerykańskim centrum operacji SWIFT w toku zwykłych prac. Mimo że dane te mogą podlegać nieznacznemu przetwarzaniu — przez co rozumie się opisane w niniejszym dokumencie bardzo ograniczone sposoby ich przeszukiwania lub odzyskiwania na użytek walki z terroryzmem — dane z komunikatów o poszczególnych transakcjach zawarte w przeszukiwalnej bazie danych nie są zmieniane, fałszowane, uzupełniane ani usuwane.

Program okazał się bardzo skutecznym narzędziem dochodzeniowym i w istotny sposób przyczynił się do ochrony obywateli USA oraz innych osób na całym świecie, a także do zapewnienia bezpieczeństwa Stanom Zjednoczonym i innym państwom. Program jest bardzo pomocny przy identyfikowaniu i ujmowaniu terrorystów i osób wspierających ich finansowo oraz daje wiele wskazówek, które są przekazywane specjalistom ds. walki z terroryzmem pracującym dla organów wywiadowczych i organów ochrony porządku publicznego na całym świecie.

Obawy zgłaszane przez Unię Europejską

Po tym jak w czerwcu 2006 roku media poinformowały opinię publiczną o istnieniu programu TFTP, w UE zaczęto wyrażać obawy z nim związane; dotyczyły one zwłaszcza faktu, że Departament Skarbu mógłby mieć dostęp do danych osobowych osoby fizycznej, której tożsamość jest znana lub której tożsamość można ustalić, zawartych w przetwarzanych przez SWIFT informacjach o transakcjach finansowych. Podniesiono zwłaszcza kwestię zgodności programu z wymogami dyrektywy o ochronie danych (dyrektywa 95/46/WC Parlamentu Europejskiego i Rady z dnia 24 października 1995 r. w sprawie ochrony osób fizycznych w zakresie przetwarzania danych osobowych i swobodnego przepływu tych danych) oraz z ustawodawstwem państw członkowskich wdrażającym tę dyrektywę.

Charakter danych SWIFT

Zapisy transakcji finansowych udostępniane przez SWIFT na mocy wezwania administracyjnego mogą obejmować informacje, które pozwalają zidentyfikować zleceniodawcę lub beneficjenta transakcji, w tym nazwisko, numer rachunku bankowego, adres, numer w krajowym systemie ewidencji ludności oraz inne dane osobowe. Jest bardzo mało prawdopodobne, by zapisy transakcji finansowych SWIFT zawierały dane szczególnie chronione, o których mowa w art. 8 dyrektywy 95/46/WE (tj. dane osobowe ujawniające pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub filozoficzne, przynależność do związków zawodowych, dane o zdrowiu lub życiu seksualnym konkretnej osoby).

Międzynarodowe zasady walki z finansowaniem działalności terrorystycznej

Dane finansowe SWIFT wykorzystywane w programie TFTP są wyjątkowo cenne w walce ze światowym terroryzmem i z finansowaniem działań terrorystycznych, a także w wypełnianiu rządowego obowiązku ochrony społeczeństwa, w zapewnianiu bezpieczeństwa narodowego oraz w wykrywaniu przestępstw terrorystycznych, prowadzeniu dochodzeń w ich sprawie, zapobieganiu im i ściganiu ich sprawców.

Społeczność międzynarodowa i władze krajowe zdają sobie sprawę z tego, że dla terrorystów środki finansowe są nieodzowne. Wyrażono to w międzynarodowej konwencji ONZ z 1999 roku o zwalczaniu finansowania terroryzmu oraz w licznych rezolucjach ONZ na temat zapobiegania finansowaniu działań terrorystycznych i na temat zwalczania tego zjawiska, a zwłaszcza w rezolucji nr 1373 Rady Bezpieczeństwa ONZ. W Stanach Zjednoczonych Departament Skarbu i Kongres utworzyły w 2004 roku Biuro Wywiadu Terrorystycznego i Finansowego, po to by ukierunkować działalność departamentu związaną z egzekwowaniem prawa i z wywiadem na dwa bliźniacze cele: ochronę systemu finansowego przed nielegalnymi działaniami oraz zwalczanie m.in. terrorystów i innych zagrożeń bezpieczeństwa narodowego. Poszczególne działy biura gromadzą i analizują informacje otrzymywane od organów ochrony porządku publicznego, organów wywiadowczych i finansowych na temat tego, w jaki sposób terroryści (i inni przestępcy) zdobywają, przekazują i przechowują środki finansowe. Dzięki tego typu działalności biuro może zamrażać aktywa należące do terrorystów, ogólnie — zwalczać terroryzm oraz wypracowywać i upowszechniać w USA i na świecie standardy walki z finansowaniem działalności terrorystycznej.

Takie i inne inicjatywy są reakcją na zwykły fakt, że terroryści są uzależnieni od regularnych przepływów gotówki, która pozwala im opłacić współpracowników, przygotowywać podróże, szkolić nowych członków grup, fałszować dokumenty, płacić łapówki, nabywać broń i organizować zamachy. Przesyłając pieniądze w systemie bankowym, często dostarczają informacji, w których zawarte są konkretne wskazówki mogące przyspieszyć dochodzenia w sprawie terroryzmu. To dlatego urzędnicy odpowiedzialni za walkę z terroryzmem przywiązują dużą wagę do finansowych danych wywiadowczych — uzyskanych m.in. dzięki programom takim jak TFTP — które okazały się bezcenne w walce ze światowym terroryzmem.

To także dlatego branży finansowej postawiono szczegółowe wymogi w zakresie przechowywania danych oraz sprawozdawczości, opracowane po to, by wspierały wysiłki rządu w dziedzinie walki z terroryzmem. Państwa na całym świecie umożliwiły to odpowiednimi aktami prawnymi, zgodnie z zaleceniami Grupy Zadaniowej ds. Finansowych. Na przykład w Stanach Zjednoczonych podstawowym umocowaniem prawnym jest ustawa o tajemnicy bankowej. W Europie podobne przepisy wprowadzono do ustawodawstwa krajowego zgodnie z trzecią dyrektywą o praniu pieniędzy, a ostatnio rozporządzeniem (WE) nr 1781/2006 Parlamentu Europejskiego i Rady z dnia 15 listopada 2006 r. w sprawie informacji o zleceniodawcach, które towarzyszą przekazom pieniężnym.

Podstawa prawna umożliwiająca uzyskiwanie i wykorzystywanie danych SWIFT

Wezwania skierowane do SWIFT są oparte na długoletnich podstawach prawnych i na powiązanym z nimi dekrecie o walce z terroryzmem i z finansowaniem działań terrorystycznych. Ustawa z 1977 roku o uprawnieniach gospodarczych na wypadek międzynarodowej sytuacji nadzwyczajnej upoważnia prezydenta Stanów Zjednoczonych do tego, by podczas sytuacji nadzwyczajnej w kraju badał transfery bankowe oraz inne transakcje, w których w jakikolwiek sposób uczestniczą cudzoziemcy. Podobnie ustawa z 1945 roku o członkostwie w ONZ upoważnia prezydenta do tego, by podczas wprowadzania w życie rezolucji Rady Bezpieczeństwa ONZ badał powiązania gospodarcze lub sposoby komunikacji cudzoziemców ze Stanami Zjednoczonymi.

W dniu 23 września 2001 r. prezydent, opierając się na obu wspomnianych ustawach oraz na rezolucjach Rady Bezpieczeństwa ONZ skierowanych przeciwko talibom i Al Kaidzie, wydał dekret nr 13224. Ogłosił w nim w kraju stan wyjątkowy w związku z zamachami z 11 września oraz z ciągłą i bezpośrednią groźbą kolejnych zamachów i zablokował mienie osób prowadzących działalność terrorystyczną, grożących jej prowadzeniem lub wspierających terroryzm; zakazał też przeprowadzania z nimi wszelkich transakcji.

Na użytek dekretu nr 13224 w sekcji 3 zamieszczono następującą definicję:

termin „terroryzm" oznacza działalność, która

(i) obejmuje akt przemocy lub akt zagrażający życiu ludzkiemu, mieniu lub infrastrukturze i która

(ii) wydaje się mieć na celu

A) zastraszenie ludności cywilnej lub wywarcie na nią nacisku;

B) wpłynięcie na politykę rządu poprzez zastraszenie lub nacisk; lub

C) wpłynięcie na postępowanie rządu poprzez dokonanie masowych zniszczeń, zabójstwa, porwania lub wzięcie zakładników.

W sekcji 7 dekretu prezydent upoważnia sekretarza Departamentu Skarbu do wykorzystania wszystkich niezbędnych uprawnień przyznanych prezydentowi dwiema wyżej wymienionymi ustawami, by zrealizować cele dekretu. Upoważnia sekretarza skarbu także do przekazania każdej ze wspomnianych funkcji innym amerykańskim urzędnikom i agencjom rządowym oraz zaleca wszystkim amerykańskim agencjom rządowym przedsięwzięcie wszelkich stosownych środków, które leżą w ich gestii, by wykonać przepisy dekretu. Ustawa o uprawnieniach gospodarczych oraz wspomniany dekret, wprowadzane w życie rozporządzeniami o sankcjach związanych ze światowym terroryzmem, dają dyrektorowi Biura ds. Kontroli Aktywów Zagranicznych, podległego Departamentowi Skarbu, prawo wystąpienia do dowolnej osoby o dostarczenie danych na temat transakcji finansowych lub danych innego rodzaju w związku z dochodzeniem w sprawie sankcji gospodarczych. To właśnie na podstawie tych aktów prawnych Biuro ds. Kontroli Aktywów Zagranicznych skierowało do SWIFT wezwania do udostępnienia danych finansowych związanych z dochodzeniami w sprawie terroryzmu.

Kontrola dostępu i bezpieczeństwo systemu informatycznego

Jak przewidują amerykańskie rządowe procedury postępowania z informacjami związanymi z dochodzeniem w sprawie terroryzmu oraz bardziej ogólnie — w sprawie finansowania działań terrorystycznych, dane uzyskane od SWIFT podlegają surowym środkom technicznym i organizacyjnym, które mają chronić informacje przed przypadkowym lub bezprawnym zniszczeniem, zaginięciem, zmodyfikowaniem lub dostępem. Wszystkie wymienione dalej środki bezpieczeństwa podlegają niezależnej kontroli.

Dane SWIFT są przechowywane w bezpiecznym miejscu, oddzielone od pozostałych danych, a systemy informatyczne są wyposażone w bardzo skuteczne zabezpieczenia przed niepożądaną ingerencją oraz w inne rodzaje ochrony, które sprawiają, że dostęp do danych możliwy jest wyłącznie w przypadkach opisanych w niniejszym dokumencie. Nie tworzy się kopii danych SWIFT, chyba że na wypadek konieczności ich odzyskania w razie awarii. Dostęp do danych oraz urządzenia komputerowe przysługują jedynie osobom, które zostały odpowiednio sprawdzone pod względem bezpieczeństwa. Nawet one mają dostęp do danych SWIFT tylko w trybie odczytu. Program TFTP przewiduje ścisłą zasadę ograniczonego dostępu — dostęp przysługuje tylko analitykom zajmującym się dochodzeniami w sprawie terroryzmu oraz osobom odpowiadającym za wsparcie techniczne programu TFTP, zarządzanie nim i nadzór nad nim.

Ekstrakcja i wykorzystywanie danych tylko na użytek dochodzeń w sprawie terroryzmu

Program TFTP nie przewiduje eksploracji danych ani żadnej innej odmiany ich algorytmicznego lub automatycznego profilowania bądź ich filtrowania komputerowego. W programie zapisano wielokrotne ścisłe kontrole, które służą temu, by ograniczyć gromadzone informacje, zagwarantować, że będą one ekstrahowane i wykorzystywane jedynie na użytek walki z terroryzmem, oraz by chronić prywatność osób niezwiązanych z terroryzmem ani z finansowaniem działań terrorystycznych. Te pokrywające się zabezpieczenia stale zawężają i znacznie ograniczają zarówno możliwość dostępu do danych finansowych przetwarzanych przez SWIFT w trakcie codziennych operacji, jak i możliwość ich wykorzystywania.

Podstawowym założeniem jest to, by wezwania kierowane do SWIFT były starannie i jak najściślej dostosowane do potrzeb, a tym samym ilość danych pozyskiwanych przez Departament Skarbu — ograniczona. SWIFT ma dostarczać Departamentowi Skarbu tylko takich danych, które departament ten uznaje za niezbędne na użytek walki z finansowaniem działań terrorystycznych, a ocenę tę wysnuwa z wcześniejszych analiz, a zwłaszcza z rodzaju komunikatów i z danych geograficznych, a także z dostrzeganych zagrożeń i podatności na nie. Ponadto kwerendy są ściśle ukierunkowane, tak by ograniczyć do minimum uzyskiwanie przekazów nieistotnych dla dochodzeń w sprawie terroryzmu. Dane udostępniane przez SWIFT przeszukuje się, by uzyskać jedynie takie informacje, które są związane z konkretnym, prowadzonym już dochodzeniem w sprawie terroryzmu. Oznacza to, że każda prowadzona kwerenda musi się odbywać na podstawie konkretnych, zarejestrowanych i udokumentowanych dowodów, które świadczą o związkach danej osoby z terroryzmem lub z finansowaniem działań terrorystycznych. Każda kwerenda danych SWIFT dokonywana w ramach programu TFTP jest jednocześnie rejestrowana — wraz z niezbędnym uzasadnieniem potwierdzającym podejrzenia o terroryzm.

W związku z przewidzianymi zabezpieczeniami dostęp do danych był możliwy jedynie w przypadku znikomej części (tj. dużo mniej niż jednego procenta) komunikatów przekazanych przez SWIFT Departamentowi Skarbu, a był możliwy tylko dlatego, że informacje te bezpośrednio odpowiadały ściśle określonym kwerendom związanym z terroryzmem.

Niezależny nadzór

Poza stałymi działaniami kontrolnymi wykonywanymi przez Departament Skarbu i przedstawionymi w niniejszym dokumencie program TFTP przewiduje różnorakie, uzupełniające się rodzaje niezależnego nadzoru: ze strony przedstawicieli samego SWIFT, niezależnej firmy audytorskiej oraz innych niezależnych organów rządu USA, w tym Kongresu.

SWIFT i zatrudnieni przez niego audytorzy zewnętrzni niezależnie nadzorują realizację programu TFTP na kilka uzupełniających się sposobów. Po pierwsze, niektórzy przedstawiciele SWIFT zostali odpowiednio sprawdzeni pod względem bezpieczeństwa i mają całodobowy dostęp do wyposażenia i danych oraz możliwość monitorowania — w czasie rzeczywistym i późniejszym — sposobu, w jaki dane są wykorzystywane, tak by mogli być pewni, że dostęp do nich ma służyć wyłącznie walce z terroryzmem. Ponadto przedstawiciele SWIFT mogą natychmiast przerwać każdą kwerendę, a nawet wyłączyć cały system, jeśli mają jakiekolwiek zastrzeżenia.

Jeżeli chodzi o niezależnych audytorów zewnętrznych, przechowywanie danych SWIFT, dostęp do nich oraz ich wykorzystanie podlegają stałym okresowym niezależnym audytom na mocy dokładnie opracowanych protokołów zgodnych z międzynarodowymi normami audytu. Przedmiotem audytów są: kontrola dostępu, zabezpieczenia systemów informatycznych oraz ograniczenie wykorzystywania danych do celów dochodzeń w sprawie terroryzmu, jak opisano powyżej. Niezależni audytorzy przekazują sprawozdania z audytu komisji ds. audytu i finansów w zarządzie SWIFT.

Ponadto, zgodnie z prawem USA, informacje o programie TFTP i jego realizacji były i będą systematycznie przekazywane rożnym komisjom Kongresu. Program TFTP był także tematem przesłuchań w Kongresie.

Poza tym nadzór nad realizacją programu TFTP sprawuje także Zarząd Nadzoru nad Prywatnością i Wolnościami Obywatelskimi, utworzony na mocy ustawy z 2004 roku o reformie wywiadu i zapobieganiu terroryzmowi. Zarząd ma za zadanie dopilnować, by obawy dotyczące poszanowania prywatności i wolności obywatelskich były odpowiednio uwzględniane podczas wprowadzania w życie amerykańskich ustaw i rozporządzeń oraz podczas realizowania przez władzę wykonawczą strategii mających chronić Stany Zjednoczone przed terroryzmem. Zarząd jest także odpowiedzialny za weryfikowanie procedur wymiany informacji na temat terroryzmu przez departamenty i agencje władz wykonawczych, po to by ustalić, czy przestrzega się wytycznych opracowanych z myślą o odpowiedniej ochronie prywatności i wolności obywatelskich.

Jak opisano poniżej, oprócz wspomnianego szerokiego niezależnego nadzoru dostęp do informacji uzyskanych z zapisów finansowych SWIFT ogranicza także restrykcyjna kontrola rozpowszechniania tych informacji, co jeszcze bardziej służy ochronie prywatności.

Wymiana informacji i ich rozpowszechnianie

Społeczność międzynarodowa uznała za szczególnie ważne dzielenie się informacjami na temat terroryzmu. Na przykład w rezolucji nr 1373 Rady Bezpieczeństwa ONZ wezwano wszystkie państwa do znalezienia sposobów, by zintensyfikować i przyspieszyć wymianę informacji operacyjnych na temat terroryzmu oraz by wymieniać informacje i w ten sposób zapobiegać dokonywaniu aktów terrorystycznych. Podobnie sekcja 6 dekretu nr 13224 nakłada na sekretarza skarbu (i innych urzędników) obowiązek dołożenia wszelkich starań, by prowadzić współpracę i koordynować działania z innymi krajami w celu zrealizowania założeń dekretu, do których należy m.in. zapobieganie aktom terroryzmu i ich tłumienie, odmawianie finansowania i świadczenia usług finansowych terrorystom oraz wymiana danych wywiadowczych na temat finansowania działań terrorystycznych. To właśnie na tej podstawie informacje zaczerpnięte z danych SWIFT są w razie potrzeby udostępniane partnerom krajowym i międzynarodowym. Podobnie jak wszystkie inne elementy programu TFTP, tak i wymiana informacji jest zgodna z prawem USA i podlega pewnym zabezpieczeniom przewidzianym, by chronić dane SWIFT oraz prywatność osób, których mogą one dotyczyć.

Analitycy ds. walki z terroryzmem prowadzący kwerendy w ramach programu TFTP weryfikują adekwatność wszelkich informacji uzyskanych w odpowiedzi na zapytanie, zanim jeszcze informacje te zostaną przygotowane do rozpowszechnienia bezpiecznymi kanałami. Departament Skarbu sprawuje także pierwotną kontrolę nad wszelkim dalszym rozpowszechnianiem informacji, co oznacza, że żadnemu odbiorcy nie wolno bez wyraźnej zgody tego departamentu dalej rozpowszechniać uzyskanych informacji. W związku z tym, podobnie jak w przypadku bezprawnego dostępu do danych SWIFT, wszelkie bezprawne ujawnienie informacji uzyskanych w ramach programu TFTP może skutkować surowymi działaniami dyscyplinarnymi bądź sankcjami cywilnymi lub karnymi.

Informacje zaczerpnięte z danych SWIFT można — pod ścisłą kontrolą — udostępniać innym amerykańskim agencjom wywiadowczym lub agencjom ochrony porządku publicznego wyłącznie po to, by mogły je wykorzystać na użytek dochodzeń w sprawie terroryzmu lub w sprawie finansowania działań terrorystycznych, wykrywania tych zjawisk, zapobiegania im lub ścigania ich sprawców lub na użytek powiązanych z tym dalszych dochodzeń i aktów oskarżenia. Wymianę informacji umożliwiają: ustawa o bezpieczeństwie narodowym, ustawa z 2004 roku o reformie wywiadu i zapobieganiu terroryzmowi oraz szereg protokołów ustaleń i pokrewnych dekretów. Agencje, które otrzymują informacje, są zobowiązane podobnie jak Departament Skarbu — na mocy prawa USA — do ochrony informacji uzyskanych w ramach programu TFTP. Należy także odnotować, że informacje uzyskane w ramach programu TFTP są przekazywane innym agencjom USA jedynie jako wskazówki, co ogranicza możliwość ich wykorzystania jako materiału dowodowego w postępowaniu sądowym. Agencje, które otrzymują informacje, opierają się na obowiązujących je podstawach prawnych, by prowadzić dochodzenia, w tym uzyskiwać dokumentację z innych źródeł mogącą później posłużyć za dowód w postępowaniu sądowym.

Te agencje rządowe dzielą się informacjami zaczerpniętymi z danych SWIFT ze swoimi zagranicznymi partnerami w tych samych celach i za każdorazową aprobatą Departamentu Skarbu, jeżeli celem jest ochrona bezpieczeństwa kraju lub egzekwowanie prawa. Wiele wskazówek uzyskanych dzięki programowi TFTP przekazano władzom zagranicznym, nie zdradzając przy tym z zasady, że źródłem jest ten właśnie program.

Jeżeli chodzi o ewentualne upublicznianie danych SWIFT, Departament Skarbu traktuje je jako poufne informacje gospodarcze, objęte klauzulą tajności, szczególnie chronione z uwagi na egzekwowanie prawa. A zatem nie upublicznia ich ani nie zamierza tego zrobić, chyba że tak nakaże prawo. W związku z jakimkolwiek postępowaniem administracyjnym lub sądowym wszczętym na wniosek strony trzeciej, która chce uzyskać dostęp do danych programu TFTP i która powołuje się na ustawę o wolności informacji, Departament Skarbu zajmie stanowisko, że takie dane nie podlegają ujawnieniu na mocy tej ustawy.

Odszkodowanie

Ograniczony charakter danych w pojedynczych komunikatach SWIFT o transakcji, zawężony dostęp do niektórych danych SWIFT w ramach programu TFTP w przypadku toczącego się dochodzenia w sprawie terroryzmu oraz obostrzenia w rozpowszechnianiu tych informacji jako wskazówek znacznie zmniejszają potrzebę zaplanowania w programie mechanizmu odszkodowawczego. Mimo to prawo USA przewiduje odpowiednie odszkodowanie za ewentualne nadużycia ze strony organów rządowych.

Jeżeli chodzi o interesy konkretnej osoby fizycznej w przypadku wykorzystania danych oraz o możliwość wniesienia o odszkodowanie za ewentualne nadużycia, należy rozróżnić przeszukiwalne dane udostępnione przez SWIFT i informacje wyekstrahowane na użytek dochodzenia w sprawie terroryzmu mogące posłużyć za podstawę decyzji administracyjnej lub innego działania ze strony rządu. Dane uzyskane od SWIFT na mocy wezwań składają się z kopii komunikatów o przeprowadzonych transakcjach finansowych, tj. z elektronicznych kopii zapisów o działalności gospodarczej przechowywanych w amerykańskim oddziale SWIFT w toku zwykłych prac. Mimo że dane te mogą podlegać nieznacznemu przetwarzaniu — przez co rozumie się opisane w niniejszym dokumencie bardzo ograniczone sposoby ich przeszukiwania lub odzyskiwania na użytek walki z terroryzmem — dane z komunikatów o poszczególnych transakcjach zawarte w przeszukiwalnej bazie danych nie są zmieniane, fałszowane, uzupełniane ani usuwane.

Ponadto należy podkreślić, że zdecydowanej większości uzyskanych od SWIFT komunikatów o transakcjach nigdy nikt nie zobaczy, nawet analitycy ds. walki z terroryzmem, a więc pozostanie ona nieznana. A zatem odpowiedź na zapytanie na temat ochrony prywatności wystosowane przez osobę fizyczną chcącą się dowiedzieć, czy informacje o niej są zawarte w bazie danych, wymagałaby prawie we wszystkich przypadkach dotarcia do danych, do których nigdy by nie dotarto podczas zwykłych operacji prowadzonych w ramach programu TFTP. Dostęp taki byłby niezgodny z wymogami programu, który przewiduje, że każda kwerenda musi mieć uprzedni związek z terroryzmem. I dodatkowo — ponieważ dane zawarte w przeszukiwalnej bazie danych nie są zmieniane, fałszowane, uzupełniane ani skreślane, nie ma powodów, by jakiekolwiek informacje korygować. Ponadto prowadziłoby to do zmiany zapisów o przeprowadzonych transakcjach, o które to zapisy występuje w wezwaniach Biuro ds. Kontroli Aktywów Zagranicznych.

Dalsze przetwarzanie danych zawartych w konkretnym komunikacie o transakcji będzie miało miejsce jedynie w przypadku stosunkowo niewielkiej liczby informacji wyekstrahowanych z bazy danych, a mianowicie tych, które bezpośrednio odpowiadają sprecyzowanej kwerendzie związanej z terroryzmem. Po tym jak dane zostaną wyekstrahowane i poddane licznym kontrolom, które mają ograniczyć ich rozpowszechnianie tylko do przypadków walki z terroryzmem, można dochodzić odszkodowania za domniemane nadużycia, korzystając z odpowiednich procedur administracyjnych i sądowych, jeżeli chodzi o działania rządu wobec rozpowszechnionych informacji.

Możliwość ubiegania się o odszkodowanie można zilustrować przedstawionym niżej przykładem; odnosi się on do działań administracyjnych podjętych przez Biuro ds. Kontroli Aktywów Zagranicznych, by zablokować mienie na mocy rozporządzeń o sankcjach związanych ze światowym terroryzmem, które to rozporządzenia wprowadzają w życie dekret nr 13224. Konkretna osoba może wnieść o zrewidowanie decyzji biura o uznaniu jej za światowego terrorystę — daje się jej możliwość udowodnienia, że „okoliczności, w wyniku których została uznana za terrorystę, już nie zachodzą", oraz „przedstawienia argumentów lub dowodów, które według niej świadczą o tym, że podstawy do uznania jej za terrorystę były niewystarczające". Osoba uznana za terrorystę może także wnieść o sądową rewizję decyzji agencji, kierując się stosownymi przepisami ustawy o procedurze administracyjnej. Przedstawione administracyjne i sądowe sposoby ubiegania się o odszkodowanie mają zastosowanie do każdej osoby, której dotyczy decyzja rządu, niezależnie od obywatelstwa.

Okres przechowywania danych

Okres przechowywania informacji dotyczących walki z terroryzmem (i wszelkich innych) jest wypadkową wielu ściśle określonych czynników, m.in. wymogów dochodzenia, stosownych przepisów o przedawnieniu oraz przepisowych terminów rozpatrywania skarg lub wnoszenia oskarżenia. Zastosowanie i traktowanie tych i innych czynników różni się w każdej agencji i zależy od rodzaju jej konkretnych zadań i od jej misji. Dlatego okresy przechowywania niektórych rodzajów informacji związanych z terroryzmem zgromadzonych przez różne agencje są zależne od rodzaju informacji oraz dochodzenia, do którego się odnoszą.

W przypadku rządu USA harmonogramy przechowywania i usuwania zapisów agencji są zatwierdzane przez Krajowy Urząd ds. Archiwów i Rejestrów zgodnie z różnymi statutami i rozporządzeniami. Dla wszelkich zapisów, o których sądzi się, że nie mają trwałej wartości, należy wyznaczyć termin usunięcia po pewnym okresie uzależnionym od ich uzasadnionej wartości administracyjnej, podatkowej i prawnej. Czynniki brane pod uwagę przez Krajowy Urząd ds. Archiwów i Rejestrów podczas zatwierdzania okresów przechowywania danych agencji to m.in. stosowne przepisy o przedawnieniu, przepisowe terminy rozpatrywania skarg lub wnoszenia oskarżenia, możliwość oszustwa, ryzyko sporu i prawa materialne oraz statuty lub rozporządzenia przyznające lub ograniczające konkretne prawo ustawowe.

Jeżeli chodzi o okres przechowywania informacji związanych z programem TFTP, należy rozróżnić dane uzyskane od SWIFT w odpowiedzi na wezwanie oraz dane wyekstrahowane służące za podstawę decyzji administracyjnej lub innego działania rządowego.

Departament Skarbu spróbuje na bieżąco — co najmniej raz w roku — wyszukiwać i usuwać wszystkie niewyekstrahowane dane, które nie są potrzebne do realizacji celów przedstawionych w niniejszych wyjaśnieniach. Zależnie od wyników wyżej wspomnianej analizy, uzależnionej od potrzeb, wszystkie niewyekstrahowane dane uzyskane przez Departament Skarbu od SWIFT po publikacji tych wyjaśnień zostaną przez niego usunięte najpóźniej po pięciu latach od momentu wpłynięcia do departamentu. Zależnie od wyników wyżej wspomnianej analizy, uzależnionej od potrzeb, wszelkie inne niewyekstrahowane dane zostaną usunięte najpóźniej po pięciu latach od momentu publikacji niniejszych wyjaśnień.

Wyekstrahowane dane bezpośrednio odpowiadające konkretnym kwerendom w sprawie terroryzmu i poddane wielokrotnym kontrolom opisanym powyżej, które zawężają ich rozpowszechnianie do celów walki z terroryzmem, są przechowywane przez okres przewidziany przez konkretny organ rządowy dla jego własnych zapisów związanych z dochodzeniami.

Na przykład dane SWIFT wyekstrahowane w ramach programu TFTP można by wykorzystać w dochodzeniu w sprawie konkretnej osoby, po to by w razie potrzeby uznać ją za światowego terrorystę na mocy rozporządzeń o sankcjach związanych ze światowym terroryzmem, które to rozporządzenia wydało Biuro ds. Kontroli Aktywów Zagranicznych. Zgodnie z harmonogramem przechowywania zapisów sporządzonym przez to biuro i zatwierdzonym przez Krajowy Urząd ds. Archiwów i Rejestrów, jeżeli powzięto ostateczną decyzję administracyjną o uznaniu danej osoby za terrorystę (decyzja ta zostaje upubliczniona), informacja, na podstawie której powzięto tę decyzję, zostaje zachowana na stałe jako pisemny dowód na poparcie działań agencji. Dowody zostają zachowane na użytek ewentualnej rewizji administracyjnej lub prawnej, w przypadku gdy decyzja zostanie zaskarżona, a także na użytek dalszych dochodzeń związanych z terroryzmem. Jeśli natomiast podczas dochodzenia nie zapadnie wspomniana decyzja, materiały z dochodzenia zostają zniszczone na miejscu najpóźniej rok po zakończeniu dochodzenia.

Ponadto zgodnie z wyżej wspomnianymi amerykańskimi aktami prawnymi okres przechowywania wskazówek uzyskanych w ramach programu TFTP, a potem rozpowszechnionych zależy od rozporządzeń i harmonogramów obowiązujących w agencji lub rządzie, do których trafiły te wskazówki. Na przykład wszelkie uzyskane informacje wykorzystywane w akcie oskarżenia Departamentu Sprawiedliwości podlegają stosownym okresom przechowywania obowiązującym w tym departamencie.

Obecna współpraca w walce z terroryzmem

Program TFTP okazał się bardzo pomocny w zwalczaniu terroryzmu na świecie, m.in. w Europie. Rząd USA będzie w dalszym ciągu rozważnie oceniał, czy jakiekolwiek informacje uzyskane w ramach programu mogą się przyczynić do prowadzenia dochodzeń w sprawie terroryzmu lub w sprawie finansowania działań terrorystycznych, zapobiegania tym zjawiskom, ich zwalczania lub ścigania ich sprawców w jednym państwie członkowskim Unii Europejskiej lub w większej ich liczbie, i we wszystkich stosownych przypadkach będzie udostępniał te informacje w najwłaściwszy sposób odpowiednim organom.

Na dowód naszego zaangażowania w walkę ze światowym terroryzmem oraz na dowód partnerstwa w tej walce wyznaczona zostanie wybitna osobistość europejska, która potwierdzi, że program jest realizowany zgodnie z niniejszymi wyjaśnieniami i zweryfikuje kwestię ochrony danych osobowych pochodzących z UE. Dopilnuje ona przede wszystkim, czy dokonano usunięcia danych niewyekstrahowanych.

Osoba ta musi mieć odpowiednie doświadczenie oraz musi zostać sprawdzona pod względem bezpieczeństwa; zostanie ona mianowana przez Komisję Europejską w konsultacji z Departamentem Skarbu na dwuletnią odnawialną kadencję. Osoba ta będzie wykonywała swoje obowiązki w sposób całkowicie niezależny. Wykonując swoje obowiązki, nie będzie zwracała się do nikogo o wskazówki ani nie będzie takich wskazówek przyjmowała. Osoba ta nie będzie podejmować żadnych działań, które byłyby niezgodne z jej obowiązkami wynikającymi z mianowania.

Mianowana osoba będzie corocznie przekazywać Komisji pisemne sprawozdanie zawierające jej spostrzeżenia i wnioski. Komisja natomiast stosownie do potrzeb będzie przekazywać sprawozdania Parlamentowi Europejskiemu i Radzie.

Departament Skarbu zapewni mianowanej osobie dostęp, informacje i dane niezbędne do wykonywania przez nią obowiązków. Osoba ta będzie przez cały czas działała zgodnie z prawnymi wymogami dyskrecji i poufności. Praktyczne szczegóły zostaną uzgodnione z Departamentem Skarbu.

Departament Skarbu poinformuje Unię Europejską o wszelkich istotnych zmianach zabezpieczeń przedstawionych w niniejszych wyjaśnieniach oraz o przyjęciu w USA jakiegokolwiek prawodawstwa, które w istotny sposób wpływałoby na stwierdzenia zawarte w niniejszych wyjaśnieniach.

Departament będzie zabiegał o opublikowanie niniejszych wyjaśnień w Rejestrze Federalnym i wyraża zgodę na ich opublikowanie w *Dzienniku Urzędowym Unii Europejskiej*.