KOMISJA
EUROPEJSKA

Bruksela, dnia 27.11.2013 r.
COM(2013) 842 final

KOMUNIKAT KOMISJI KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Europejski system śledzenia środków finansowych należących do terrorystów (TFTS UE)

{SWD(2013) 488 final}
{SWD(2013) 489 final}

KOMUNIKAT KOMISJI KOMUNIKAT KOMISJI DO PARLAMENTU EUROPEJSKIEGO I RADY

Europejski system śledzenia środków finansowych należących do terrorystów (TFTS UE)

W ślad za komunikatem z dnia 13 lipca 2011 r. (COM (2011) 429) celem niniejszego komunikatu jest poinformowanie Parlamentu Europejskiego i Rady o wynikach przeprowadzonej analizy dotyczącej wykonalności utworzenia europejskiego systemu śledzenia środków finansowych należących do terrorystów (TFTS UE).

1. KONTEKST

1.1. Geneza wniosku i definicja

Podczas negocjacji poprzedzających zawarcie umowy UE-USA w sprawie TFTP[1] miały miejsce rozmowy na temat najlepszego sposobu ochrony danych osobowych i przestrzegania praw podstawowych w kontekście tejże umowy. Niektóre strony twierdziły, że pobieranie danych na terytorium europejskim ograniczyłoby ilość danych przekazywanych do Stanów Zjednoczonych i zapewniłoby wyższy poziom gwarancji w zakresie ochrony danych. Niektóre państwa członkowskie były zdania, że utworzenie niezależnego europejskiego systemu śledzenia źródeł finansowania terroryzmu stanowi wartość dodaną w perspektywie długoterminowej. Parlament Europejski zwrócił się do Rady i Komisji o podjęcie wszelkich niezbędnych kroków do opracowania trwałego, uzasadnionego prawnie europejskiego rozwiązania kwestii pobierania żądanych danych na terytorium europejskim. Rada i Parlament Europejski, wyrażając zgodę na zawarcie umowy UE-USA w sprawie TFTP, wezwały Komisję do przedłożenia w ciągu jednego roku od daty wejścia w życie umowy warunków prawnych i technicznych pobierania danych na terytorium UE, a w ciągu trzech lat od daty wejścia w życie umowy do przedstawienia sprawozdania z postępu prac nad tworzeniem równoważnego systemu unijnego[2]. Ponadto art. 11 umowy UE-USA w sprawie TFTP stanowi, że w trakcie obowiązywania umowy Komisja przeprowadzi badanie na temat możliwego wprowadzenia równoważnego unijnego systemu pozwalającego na bardziej ukierunkowane przekazywanie danych.

Dla celów niniejszego komunikatu równoważny system unijny należy odróżniać od warunków ramowych dla pobierania danych na terytorium UE. Pod pojęciem *warunki ramowe dla pobierania danych* na terytorium UE należy rozumieć system umożliwiający

[1] Dz.U. L 195 z 27.7.2010, s. 5.
[2] Decyzja Rady z 13 lipca 2010 r., Dz.U. L 195 z 27.7.2010, s. 3.

wyszukiwanie danych przekazywanych obecnie przez UE Stanom Zjednoczonym, które ma być prowadzone na terytorium UE. Natomiast *równoważny system UE* byłby niezależnym europejskim systemem śledzenia źródeł finansowania terroryzmu poprzez dostęp do danych wskazanego dostawcy lub dostawców, wyszukiwanie tych danych i ich analizę. Utworzenie unijnego systemu wymagałoby zmiany umowy UE-USA w sprawie TFTP.

1.2. Podjęte kroki

W grudniu 2010 r. Komisja zleciła wykonanie *badania*, które zostało przedłużone w lipcu 2011 r., tak by objąć dodatkowy wariant systemu przechowywania i pobierania danych. W trakcie tego badania Komisja uczestniczyła w czterech spotkaniach z udziałem ekspertów zainteresowanych stron, takich jak Europol, Europejski Inspektor Ochrony Danych, wyznaczony dostawca w ramach programu TFTP[3], oraz wielu ekspertów z państw członkowskich reprezentujących zainteresowane ministerstwa, organy ścigania i agencje wywiadowcze, a także organy właściwe do spraw ochrony danych.

W dniu 13 lipca 2011 r. Komisja przedstawiła w *komunikacie do Parlamentu Europejskiego i Rady („komunikat z 2011 r.")* pięć możliwych wariantów dla europejskiego systemu śledzenia środków finansowych należących do terrorystów („TFTS UE"). Trzy z nich zostały uznane za wykonalne. Celem komunikatu z 2011 r. było rozpoczęcie debaty w sprawie dalszych działań i zebranie opinii, które zostaną wykorzystane do przeprowadzenia oceny skutków.

Kwestie tę przedstawiono w październiku 2011 r. na posiedzeniach Rady ds. Wymiaru Sprawiedliwości i Spraw Wewnętrznych oraz Komisji Wolności Obywatelskich Parlamentu Europejskiego.

Ponieważ państwa członkowskie i Parlament Europejski nie wyraziły wyraźnej preferencji na korzyść któregoś z tych wariantów, podjęto decyzję o uwzględnieniu wszystkich tych wariantów w ocenie skutków Komisji oraz o dalszej pracy nad nimi poprzez opracowywanie różnych wariantów szczegółowych. Niniejszy komunikat opiera się na ocenie skutków[4].

[3] Stowarzyszenie Międzynarodowej Teletransmisji Danych Finansowych (SWIFT)
[4] SWD 2013 (xx) z dnia

2. GŁÓWNE ZASADY KOMISJI ORAZ ZIDENTYFIKOWANE WARIANTY

2.1. Zasady strategii zarządzania informacjami przyjęte w czasie prezydencji szwedzkiej

W analizie dotyczącej proponowanych dalszych działań Komisja bierze pod uwagę podstawowe zasady zawarte w wydanej w 2009 r. strategii zarządzania informacjami[5], uwzględnione później i dalej rozwijane w komunikatach Komisji w sprawie przeglądu zarządzania informacjami w przestrzeni wolności, bezpieczeństwa i sprawiedliwości w 2010 r.[6] oraz w sprawie europejskiego modelu wymiany informacji w 2012 r.[7].

Istotne znaczenie w tym względzie mają zasady ochrony praw podstawowych, konieczności, proporcjonalności i efektywności pod względem kosztów.

Ochrona *praw podstawowych* zagwarantowanych w Karcie praw podstawowych Unii Europejskiej, w szczególności prawa do prywatności i ochrony danych osobowych, jest jednym z głównych aspektów, którymi kieruje się Komisja przy opracowywaniu nowych wniosków dotyczących przetwarzania danych osobowych w dziedzinie bezpieczeństwa wewnętrznego. W art. 7 i 8 Karty zapisano prawo każdego człowieka do „poszanowania życia prywatnego i rodzinnego" i „ochrony danych osobowych, które go dotyczą". W art. 16 Traktatu o funkcjonowaniu Unii Europejskiej, który jest wiążący dla państw członkowskich oraz instytucji, agencji i organów Unii, podkreślono ponownie prawo każdej osoby „do ochrony danych osobowych jej dotyczących". Zgodnie z art. 52 Karty, z zastrzeżeniem zasady proporcjonalności, ograniczenia w korzystaniu z praw i wolności uznanych w karcie mogą być wprowadzone wyłącznie wtedy, gdy są konieczne i rzeczywiście odpowiadają celom interesu ogólnego uznawanym przez Unię lub potrzebom ochrony praw i wolności innych osób.

Ingerencję w prawo do prywatności uważa się za *konieczną*, jeśli jest ona uzasadniona pilną potrzebą, jest proporcjonalna do wyznaczonego celu oraz jeśli przyczyny podane przez władzę publiczną dla jej uzasadnienia są odpowiednie i wystarczające.

Mimo iż trudno jest zmierzyć wszystkie koszty terroryzmu w aspekcie finansowym, obowiązuje zasada *efektywności od względem kosztów*. Podejście polegające na *efektywności pod względem kosztów* uwzględnia istniejące już rozwiązania, tak by maksymalnie

[5] Konkluzje Rady z dnia 30 listopada 2009 r. na temat strategii zarządzania informacjami do celów ochrony bezpieczeństwa wewnętrznego UE 16637/09.
[6] COM(2010) 385 z 20 lipca 2010 r.
[7] COM(2012) 735, 7 grudnia 2012 r.

zmniejszyć dublowanie pracy oraz osiągnąć największą możliwą synergię. Konieczne jest przeprowadzenie oceny możliwości osiągnięcia celu wyznaczonego we wniosku poprzez lepsze wykorzystanie istniejących instrumentów.

2.2. Podejście

W świetle zasad, o których mowa powyżej, Komisja zbadała, czy system TFTS UE byłby konieczny i proporcjonalny w stosunku do jego kosztów, korzyści i jego wpływu na prawa podstawowe w porównaniu ze stanem obecnym.

Jeśli chodzi o *korzyści*, system unijny mógłby przyczynić się do zwiększenia możliwości dostępu UE i jej państw członkowskich do odpowiednich danych i mógłby wzmocnić ich zdolności analityczne do śledzenia i identyfikacji terrorystów poprzez transakcje finansowe. Ponieważ transakcje finansowe mogą dostarczyć cennych danych, które mogą być niedostępne z innych źródeł, narzędzie to byłoby szczególnie wartościowe dla wykrywania działań terrorystycznych i uczestniczących w nich osób. W związku z tym system TFTS UE mógłby stanowić dodatkowy instrument pozyskiwania informacji i pracy dochodzeniowej prowadzenia dochodzeń w ramach walki z terroryzmem i na rzecz zwiększania bezpieczeństwa w UE, w szczególności wówczas, gdy system taki miałby objąć większą liczbę dostawców danych finansowych i rodzajów transakcji. Należy jednak wyważyć korzyści płynące z systemu TFTS UE z szacunkowymi kosztami wprowadzenia i utrzymania takiego systemu, w tym z obciążeniami finansowymi dla UE, państw członkowskich oraz dla wyznaczonych dostawców przedmiotowych danych.

2.3. Przedstawienie wariantów

Wzięto pod uwagę szereg wariantów dotyczących zarówno *warunków ramowych dla pozyskiwania* danych na terytorium UE, jak i *równoważnego systemu unijnego*.

2.3.1. Ramy dla pozyskiwania danych na terytorium UE

Ramy dla pobierania danych na terytorium UE mogłyby być realizowane w formie systemu zatrzymywania i pobierania danych przechowywanych przez wyznaczonego dostawcę, umożliwiającego bezpośredni dostęp do danych, które są aktualnie przekazywane Stanom Zjednoczonym w ramach umowy w sprawie TFTP. Taki bezpośredni dostęp mieliby analitycy lub eksperci z USA posiadający odpowiednie upoważnienie do tego celu.

W ramach tego wariantu jedną z możliwości byłoby zatrzymywanie danych na serwerze wyznaczonego dostawcy przez pewien okres czasu i prowadzenie przeszukiwania bezpośrednio na tym serwerze. Obecny dostawca wyznaczony w ramach umowy UE-USA w

sprawie TFTP stosuje jednak silne środki ochrony i bezpieczeństwa danych, które nie pozwalają na identyfikację osób, o których mowa w komunikacie, w związku z tym prowadzenie przeszukiwania opartego na danych osobowych w jego aktualnej bazie danych nie jest możliwe. Niezbędne byłoby zatem utworzenie odrębnej bazy danych.

Alternatywnie, dane mogłyby być wyodrębniane i przechowywane w innym bezpiecznym miejscu w UE. Analitycy lub eksperci z USA upoważnieni do przeprowadzania przeszukiwań mogliby albo być umiejscowieni fizycznie w siedzibie wyznaczonego dostawcy, albo mieć zdalny dostęp do danych. W każdym wypadku, niezależnie od lokalizacji danych, należałoby zadbać o kompleksowe i solidne środki zabezpieczające, dostosowane do konkretnego rozwiązania przyjętego dla struktury systemu.

2.3.2. Równoważny system unijny

W odniesieniu do utworzenia unijnego systemu równoważnego wzięto pod uwagę szereg wariantów (jak przedstawiono w komunikacie z 2011 r.), w tym system w pełni scentralizowany na poziomie UE, system zdecentralizowany na poziomie państw członkowskich oraz trzy systemy hybrydowe, w których działania odbywałyby się zarówno na poziomie UE, jak i na poziomie państw członkowskich.

W ramach każdego wariantu istnieją różne możliwości dotyczące zakresu systemu UE. Należy zdecydować, jakie rodzaje komunikatów i jacy wyznaczeni dostawcy byliby systemem objęci. W przypadku unijnego systemu równoważnego można by trzymać się rodzaju komunikatów finansowych i wyznaczonych dostawców objętych obecnie umową UE-USA w sprawie TFTP lub tez wyjść poza to ograniczenie.

- Wariant zakładający w pełni scentralizowany system na poziomie UE oznaczałby, że jedna wspólna jednostka UE wypełniałaby wszystkie kluczowe funkcje systemu: wnioskowanie o pobranie danych, zapisywanie danych, przeprowadzanie przeszukiwań danych, analiza danych, ochrona i nadzorowanie systemu oraz przekazywanie wskazówek dotyczących identyfikacji do państw członkowskich. Wariant ten jest błędny pod względem prawnym, gdyż nie byłby zgodny z art. 72 TFUE, który stanowi, że główna odpowiedzialność za utrzymanie porządku publicznego i ochronę bezpieczeństwa wewnętrznego spoczywa na państwach członkowskich. System taki nie byłby wykonalny ani możliwy do przyjęcia przez państwa członkowskie, gdyż wymagałby on utworzenia centralnej jednostki wywiadowczej na poziomie UE

- W pełni zdecentralizowany system na poziomie państw członkowskich oznaczałby, że system byłby obsługiwany przez właściwe organy państw członkowskich, zaś na poziomie UE nie byłyby realizowane żadne funkcje. W ten sposób dane mogłyby być przekazywane jednocześnie wszystkim 28 państwom członkowskim i przez nie równolegle przeszukiwane. Zwielokrotniłoby to przepływ danych i pociągnęło za sobą wysokie koszty. Zwiększyłoby się również ryzyko niespójnego traktowania danych i wprowadzania niejednolitych mechanizmów ochrony danych. W związku z tym wariantu tego nie uznaje się za realny.

Te dwa warianty zostały tym samym wyłączone z bardziej szczegółowej oceny.

Trzy pozostałe warianty unijnego systemu równoważnego polegają na rozdzieleniu poszczególnych funkcji między różne jednostki na poziomie UE oraz na poziomie krajowym („systemy hybrydowe").

Zgłaszanie zapotrzebowania danych, ich pobieranie i zapisywanie w bazie danych w bezpiecznym miejscu w UE musiałoby we wszystkich tych systemach hybrydowych odbywać się na bieżąco i za każdym razem na podstawie nowego zapytania skierowanego do wyznaczonego dostawcy lub dostawców. Właściwe przeszukiwanie odbywałoby się następnie w tej centralnej bazie danych. W przypadku wszystkich tych wariantów należałoby zadbać o odpowiednie środki w celu ochrony danych.

- A) W przypadku pierwszego systemu hybrydowego, jednostki koordynacji i dokonywania analiz w systemie TFTS UE, należałoby utworzyć centralną jednostkę na szczeblu UE. Miałaby ona za zadanie pozyskiwać dane od wyznaczonego dostawcy lub dostawców, przeprowadzać przeszukiwania i analizy danych oraz przekazywać ich wyniki. W przeciwieństwie do systemu w pełni scentralizowanego państwa członkowskie miałyby bezpośredni dostęp do systemu i mogłyby składać wnioski o przeszukanie danych, które w ich imieniu byłoby przeprowadzane przez jednostkę centralną lub przez ich własnych analityków.
- B) Drugi system hybrydowy, jednostka pobierania danych w systemie TFTS UE, również obejmowałby utworzenie unijnej jednostki centralnej. W tym wariancie jednak organ UE wykonywałby przeszukiwanie na wniosek państw członkowskich i przekazywałby państwom członkowskim wyniki bez ich analizowania. Dodatkowo organ UE mógłby przeprowadzać własne przeszukiwania oraz analizować ich wyniki.

- C) Ostatni hybrydowy system, jednostka koordynacji wydziałów wywiadu finansowego[8] („Financial Intelligence Units – FIU") przewiduje utworzenie platformy ad-hoc na poziomie UE. Nie byłoby to stały organ, lecz raczej grupa ekspertów z dziedziny wywiadu finansowego uczestniczących w posiedzeniach odbywanych w razie potrzeby. Platforma FIU mogłaby zostać do tego celu ewentualnie rozszerzona: Każde państwo członkowskie mianowałoby jednego przedstawiciela, który działałby w jego imieniu. To gremium ad-hoc zbierałoby wnioski z jednostek FIU poszczególnych państw członkowskich i na ich podstawie kierowałoby wnioski o dane do wyznaczonego dostawcy lub dostawców. Przedstawiciele państw członkowskich byliby odpowiedzialni za przeszukiwanie i analizowanie danych oraz odpowiednie przekazywanie wyników w imieniu swojego państwa członkowskiego. Następnie to rolą właściwych organów państw członkowskich byłoby wykorzystanie wskazówek wywiadowczych i ich dalsze przekazanie na szczeblu krajowym.

2.3.3. Status quo: umowa UE-USA w sprawie TFTP

Obecnie UE i państwa członkowskie mogą składać wnioski o przeszukanie danych przez USA w ramach umowy UE-USA w sprawie TFTP regulującej przetwarzanie i przekazywanie danych z komunikatów finansowych przez Unię Europejską Stanom Zjednoczonym do celów programu śledzenia środków finansowych należących do terrorystów („TFTP").

Program ten jest narzędziem przeciwdziałania terroryzmowi opracowanym przez USA po atakach terrorystycznych z 11 września 2001 r. Jego głównym elementem jest przeprowadzanie przeszukiwań danych dostarczonych przez wyznaczonego dostawcę, w tym danych przekazywanych z UE.

Umowa UE-USA w sprawie TFTP reguluje szczegółowo sposób składania wniosków o dane przez władze USA. Europol weryfikuje, czy wnioski o dane otrzymane od Stanów Zjednoczonych są zgodnie z tą umową i – w szczególności – czy są one sporządzone możliwie jak najwęziej, by ograniczyć do minimum ilość przekazywanych danych. Bezpieczne wykorzystywanie, przechowywanie i usuwanie danych jest uregulowane w szeregu postanowień umowy. Przekazane dane są przechowywane w bezpiecznym miejscu i zapisywane odrębnie od wszelkich innych danych. Umowa przewiduje pięcioletni okres zatrzymania danych oraz obowiązek przeprowadzania regularnej oceny konieczności zatrzymania danych. Dwóch z niezależnych nadzorców w Stanach Zjednoczonych zostało

[8] Decyzja Rady z dnia 17 października 2000 r. dotycząca uzgodnień w sprawie współpracy pomiędzy jednostkami wywiadu finansowego państw członkowskich w odniesieniu do wymiany informacji

wybranych przez UE. Kontrolują oni na bieżąco, jak funkcjonuje system, i mają możliwość sprawdzenia każdorazowo przeszukania danych dokonanego przez urzędników Departamentu Skarbu (USA), aby być pewnym, że przedmiot przeszukiwania danych ma związek z terroryzmem lub jego finansowaniem.

Umowa zawiera również postanowienia dotyczące prawa dostępu do danych osobowych i ich poprawiania oraz dotyczące procedur odwoławczych. Umowa stanowi, że każda osoba, która uzna, iż jej dane osobowe były przetwarzane z naruszeniem umowy, ma prawo do skorzystania ze skutecznych środków odwoławczych na drodze administracyjnej lub sądowej zgodnie z prawem – odpowiednio – Unii Europejskiej, jej państw członkowskich i Stanów Zjednoczonych. Ponadto umowa stanowi, że każda osoba, niezależnie od obywatelstwa i kraju zamieszkania, ma na mocy przepisów prawa USA dostęp do sądowych środków odwoławczych od niekorzystnych działań o charakterze administracyjnym.

Do odpowiednich przepisów regulujących środki odwoławcze od niekorzystnych działań administracyjnych Departamentu Skarbu w związku z danymi osobowymi uzyskanymi na podstawie tej umowy należą ustawa o postępowaniu administracyjnym (Administrative Procedure Act) i ustawa o wolności informacji (Freedom of Information Act). Na podstawie ustawy o postępowaniu administracyjnym osoby, które poniosły szkodę na skutek działania rządu USA, mają prawo do wniesienia środka odwoławczego przeciwko temu działaniu. Ustawa o wolności informacji pozwala osobom na wnoszenie administracyjnych i sądowych środków odwoławczych w celu uzyskania wglądu do akt rządowych. Istniejące ujednolicone procedury dostępu do danych osobowych lub ich poprawiania, usunięcia lub zablokowania, uzgodnione między Komisją, USA i Grupą Roboczą Art. 29, mają na celu ułatwienie korzystania z tych praw przez obywateli UE. Wykonanie umowy oraz przewidzianych w niej gwarancji bezpieczeństwa i kontroli podlega regularnym przeglądom na mocy art. 13 umowy. Dwa takie przeglądy przeprowadzono w latach 2011[9] i 2012[10] i uznano przy tym, że umowa została prawidłowo wykonana. Trzeci przegląd zaplanowano na wiosnę 2014 r. Wspólne sprawozdanie dotyczące wartości dostarczonych danych, przygotowane zgodnie z art. 6 umowy, przedstawia korzyści wynikające z programu TFTP w zakresie zapobiegania i przeciwdziałania terroryzmowi i jego finansowaniu oraz fakt skorzystania z programu TFTP przez szereg państw członkowskich. Informacje udostępnione w ramach TFTP, a także ich dokładność umożliwiają identyfikację i śledzenie terrorystów oraz ich sieci wsparcia na całym świecie. Rzucają one światło na istniejące struktury finansowe organizacji terrorystycznych i

[9] SEC (2011) 438 z 30 marca 2011 r.
[10] SWD (2012) 454 z 14 grudnia 2012 r.

umożliwiają wykrycie nowych strumieni wsparcia finansowego i identyfikację uczestniczących podmiotów.

3. OCENA

Przy ocenie kwestii, czy należy zaproponować utworzenie systemu TFTS UE, Komisja musi pogodzić ze sobą różne poglądy i oczekiwania dotyczące poziomu ambicji systemu UE. Cele systemu TFTS UE są różnie postrzegane przez rozmaite zainteresowane strony i decydentów. Komisja zbadała możliwości i konsekwencje obydwu scenariuszy pod kątem wyszczególnionych powyżej zasad rozwoju i wdrażania nowych inicjatyw politycznych. Przede wszystkim przy rozpatrywaniu każdego z wariantów brano pod uwagę jego konieczność, proporcjonalność i efektywność pod względem kosztów.

3.1. Ramy dla pozyskiwania danych na terytorium UE

Zgodnie z opisem w pkt 2.3.1. wariant systemu przechowywania i pobierania danych byłby sposobem na gromadzenie, przechowywanie i przeszukiwanie danych, które obecnie są przekazywane do USA w ramach umowy UE-USA w sprawie TFTP, na terytorium Unii Europejskiej. Nie stwarzałby zatem dodatkowych korzyści w zakresie wywiadu dla UE czy też państw członkowskich w porównaniu do obecnej sytuacji. Wręcz przeciwnie, biorąc pod uwagę fakt, że dane TFTP są przechowywane w USA i UE, fragmentaryzacja procesu przeszukiwania danych, który obecnie jest prowadzony na podstawie jednego zestawu danych TFTP, może mieć negatywny wpływ na jakość i liczbę wskazówek wywiadowczych oraz może zmniejszać ogólną wydajność programu TFTP. Może ona również znacząco spowolnić proces analizy, gdyż konieczne może okazać się dokonanie różnych następujących po sobie przeszukiwań danych TFTP przechowywanych w dwóch lokalizacjach w celu podjęcia dalszych działań na podstawie wskazówek wywiadowczych. Szybkość ma często zasadnicze znaczenie w przypadku dochodzeń w sprawie terroryzmu.

Pobieranie danych na terytorium Europy, a nie w Stanach Zjednoczonych, nie zagwarantowałoby samo w sobie lepszej ochrony danych osobowych. Ochrona dostępu do danych jest kluczowa dla zapewnienia prawidłowego wykorzystywania danych niezależnie od ich lokalizacji. W tym celu konieczne byłoby wdrożenie zestawu solidnych zabezpieczeń, które gwarantowałyby zgodność przetwarzania i wykorzystywania danych z niezbędnymi wymogami. Należałoby wyposażyć taki system w funkcję kontrolną odpowiedzialną za weryfikację wniosków o przeszukiwanie danych i ich uzasadnień. Niezależni nadzorcy pełniliby ważną rolę, jeśli chodzi o zagwarantowanie, że dane te wykorzystywane są do

ograniczonych celów określonych w dowolnej umowie dotyczącej utworzenia systemu. Aby zapobiec nieuprawnionemu dostępowi do danych lub ich ujawnianiu, należałoby podjąć odpowiednie środki, np. przechowywanie danych w bezpiecznym środowisku fizycznym. Konieczne byłoby wprowadzenie procedur dostępu do danych osobowych oraz ich poprawiania, a także właściwych procedur odwoławczych. Należałoby zlecić audyt zewnętrzny, by zapewnić prawidłowe funkcjonowanie systemu.

W ramach umowy UE-USA w sprawie TFTP, USA nie mają dostępu do wszystkich danych wyznaczonego dostawcy, ale jedynie do zestawów danych, o które wystąpiły, za zgodą Europolu udzieloną na podstawie przeszłych i bieżących analiz zagrożenia terroryzmem. O ile nie zostanie wprowadzony podobny mechanizm wstępnego zawężania wniosków o dane, umożliwienie bezpośredniego przeszukiwania wszystkich danych wyznaczonego dostawcy spowoduje dalszy wzrost stopnia narażenia danych i wpływu na prawa do ochrony danych. Wymagałoby to znacznej zmiany sposobu pracy wyznaczonego dostawcy oraz przechowywania jego danych. Obecnie komunikaty finansowe, które są objęte zakresem umowy, są przechowywane w formie, która nie pozwala na identyfikację osób, o których mowa w treści danych zawartych w tych komunikatach. Każdy komunikat finansowy jest zaszyfrowany, a przeszukiwanie w nim danych jest możliwe tylko według metadanych, tzn. według daty wysłania, typu komunikatu i zaangażowanego banku wysyłającego i przyjmującego. Wyznaczony dostawca wprowadził silną ochronę danych oraz mocne środki bezpieczeństwa w celu ochrony danych jego klientów na całym świecie. By umożliwić zatem przeszukiwanie danych bezpośrednio na obecnym serwerze wyznaczonego dostawcy, należałoby w pierwszej kolejności odszyfrować wszystkie komunikaty. Zakres takiej czynności byłby nadmierny i nieproporcjonalny, ponieważ wyznaczony dostawca przechowuje na serwerze więcej komunikatów niż jest wymaganych w celu zwalczania finansowania terroryzmu. Ponadto bezpośredni dostęp w celu przeszukiwania danych byłby nazbyt uciążliwy dla bieżącej działalności wyznaczonego dostawcy i stwarzałby znaczne ryzyko operacyjne i systemowe oraz zagrażałby bezpieczeństwu. W związku z tym konieczne byłoby stworzenie oddzielnej bazy danych na terytorium UE w celu przechowywania niezbędnych danych wyznaczonego dostawcy.

Konieczne byłyby znaczne inwestycje w celu wprowadzenia takiego systemu oraz zagwarantowania jego pełnej zgodności ze środkami ochrony. Należałoby dostosować pomieszczenia wyznaczonego dostawcy lub inne zabezpieczone lokalizacje do szczególnych

wymogów, opracować i stosować rozwiązania informatyczne i techniczne oraz zatrudnić i przeszkolić wykwalifikowany personel, który zarządzałby systemem i go nadzorował.

Wariant ten zakłada, że UE i państwa członkowskie ponosiłyby wszelkie niedogodności i koszty mechanizmu ustanowionego wyłącznie na potrzeby TFTP, instrumentu należącego do państwa trzeciego. Obecnie wariant ten nie wydaje się konieczny, proporcjonalny ani efektywny pod względem kosztów, ponieważ nie przyniósłby żadnych dodatkowych korzyści wywiadowczych, byłby kosztowny i trudny do wdrożenia oraz mógłby stworzyć zagrożenie dla ochrony danych osobowych.

3.2. Równoważny system unijny

W pełni scentralizowany system TFTS UE został wyłączony z bardziej szczegółowej oceny ze względu na brak podstawy prawnej i małe prawdopodobieństwo, że państwa członkowskie zaakceptowałyby scentralizowaną rolę UE w strefie ich kompetencji. W pełni zdecentralizowany system został wykluczony, ponieważ wiązałyby się z nim bardzo poważne konsekwencje w zakresie kosztów oraz miałby on zwielokrotniony wpływ na prawa do ochrony danych. Ocenione trzy systemy hybrydowe pozwoliłyby państwom członkowskim w różnym stopniu kontrolować przeszukiwanie danych, które jest realizowane przez te państwa i scentralizowany organ UE.

Rozszerzenie zakresu ekwiwalentnego systemu unijnego, tak by objął on skomputeryzowane systemy rozrachunków, e-pieniądze oraz inne dane niepochodzące z komunikatów FIN, przyniosłoby korzyści w zakresie wywiadu, gdyż zwiększyłoby zdolność UE do śledzenia płatności wewnątrzunijnych i mogłoby pomóc stworzyć bardziej przyszłościowy system aniżeli ten, który zajmuje się wyłącznie komunikatami finansowymi. Każde dodanie wyznaczonego dostawcy zwiększałoby jednak ryzyko naruszenia praw do ochrony danych i tym samym wymagałoby sztywnych warunków, zabezpieczeń i środków kontroli. Zwiększyłoby to obciążenie administracyjne po stronie wyznaczonych dostawców. Dodanie wielu dostawców danych i komunikatów w celu stworzenia takiego skomplikowanego systemu, równocześnie wymagającego pod względem technicznym i organizacyjnym, w znacznym stopniu zwiększyłoby koszty.

W wyniku tej analizy każdy realny system TFTS UE wykorzystywałby wyłącznie dane zawarte w komunikatach FIN, gdyż Komisja uważa, że dodatkowe korzyści związane z korzystaniem z wielu typów danych i dostawców nie przeważają nad znacznymi kosztami po stronie prywatnych przedsiębiorstw ani nad uszczerbkiem dla praw do prywatności i ochrony

danych, z którymi wiązałby się taki system. Jako że system UE objąłby jedynie ten sam rodzaj wyznaczonego dostawcy i rodzaj komunikatu co program TFTP, ilość i jakość uzyskanych wskazówek wywiadowczych oraz narażenie danych byłyby zatem porównywalne do programu TFTP UE-USA.

Jak wspomniano powyżej, istnieją trzy warianty takiego równoważnego systemu UE: A) Dział koordynacji i dokonywania analiz w systemie TFTS UE , B) Dział pobierania danych w systemie TFTS UE oraz C) dział koordynacji Wydziału Wywiadu Finansowego.

Wariant A mógłby mieć pozytywny wpływ na zapobieganie terroryzmowi i poprawę bezpieczeństwa w UE. Zespoły UE i państw członkowskich zajmujące się przeszukiwaniem danych i analizą wyników podjęłyby pewne kroki w celu zagwarantowania, że szczególne wymogi w zakresie wywiadu UE i państw członkowskich są w pełni brane pod uwagę oraz że system jest ukierunkowany na konkretne „zagrożenie dla UE". Poprawa ta zależy od rosnącej gotowości i zdolności państw członkowskich do wymiany informacji i analizy w perspektywie średnio- i długoterminowej. Nie jest jasne, w jakim stopniu można polegać na takim zwiększonym przepływie informacji. Ponadto, jako że państwa członkowskie zachowałyby możliwość występowania do USA o przeszukiwanie danych w ramach programu TFTP, system ten wymagałby znacznego poparcia i współpracy ze strony państw członkowskich, jeśli miałby on zapewnić bardziej spójny obraz UE.

Wariant B mógłby mieć pewien pozytywny wpływ na zapobieganie terroryzmowi i poprawę bezpieczeństwa w UE. System byłby bardziej czuły na analizy zagrożeń dla UE, ponieważ przeszukiwanie danych odbywałoby się zgodnie ze szczegółowymi wymogami wywiadowczymi państw członkowskich. Rola scentralizowanego organu unijnego ograniczałaby się jednak do przeszukiwania danych oraz przekazywania odpowiednich danych do wnioskującego państwa członkowskiego; taki organ pełniłby raczej rolę strażnika. W rezultacie nie byłoby żadnej analizy na poziomie UE, a system byłby w pełni zależny od analiz, jakie państwa członkowskie wymieniają miedzy sobą, poza systemem, jeśli miałby powstać spójny obraz wywiadowczy UE. Niezdolność systemu do zagwarantowania jednolitego podejścia do definicji przeszukiwania danych zwiększyłaby ryzyko wyników fałszywie dodatnich, tym samym naruszając prawo do ochrony danych i do prywatności.

Wariant C odpowiadałby szczególnym potrzebom państw członkowskich w zakresie wywiadu i tym samym miałby pewien pozytywny wpływ na zapobieganie terroryzmowi oraz poprawę bezpieczeństwa. Jako że krajowe jednostki wywiadu finansowego byłyby odpowiedzialne za

przeszukiwanie danych i dokonywanie analiz przez ich państwa członkowskie, wariant ten ma takie same wady co wariant B – można by osiągnąć wyraźny obraz jedynie dzięki wzmocnionej współpracy państw członkowskich, poza systemem. Ponadto jednostki wywiadu finansowego koncentrują się tylko na wywiadzie finansowym i rozdział między taką informacją a szerzej pojętą informacją wywiadowczą mógłby utrudnić dostrzeżenie powiązań i finansowania terroryzmu. Istnieje również bardzo niski poziom zaangażowania UE w ten wariant, a zdolność zwiększyłaby się głównie na poziomie krajowym.

Wszystkie wspomniane warianty pociągałyby za sobą znaczne koszty dla UE, państw członkowskich oraz wyznaczonego dostawcy, w tym między innymi koszt budowy infrastruktury informatycznej, bezpiecznych obiektów oraz koszt dziesiątek, jeśli nie setek, pracowników odpowiedzialnych za zarządzanie takim systemem i za wdrożenie zabezpieczeń i kontroli. Każdy z tych ewentualnych systemów może jednak przyczynić się do poprawy bezpieczeństwa w Europie, gdyż stosowałby oceny zagrożeń dostosowanych do potrzeb europejskich.

Niezależny instrument w zakresie wywiadu i dochodzeń na terytorium Europy pozwoliłby znieść wymóg przekazywania danych do USA. Jednak każdy system TFTS UE nadal wymagałby solidnych zabezpieczeń i odpowiedniej kontroli ochrony danych podobnych do tych, które już obowiązują w ramach umowy UE-USA w sprawie TFTP, a w każdym razie zgodnych z dorobkiem prawnym UE i państw członkowskich w dziedzinie ochrony danych. Należałoby sprawdzić, czy wszystkie wnioski o przeszukiwanie danych w systemach UE są zgodne ze ścisłym ograniczeniem do walki z terroryzmem i finansowaniem działalności terrorystycznej, w tym również czy zasadne jest przekazywanie danych. W szczególności, wykwalifikowani niezależni nadzorcy mieliby obowiązek sprawdzić, czy każde przeszukiwanie przez UE i państwo członkowskie zostało należycie zatwierdzone i było wymagane do celów zwalczania terroryzmu i jego finansowania. Należałoby zapewnić bezpieczne wykorzystywanie i przechowywanie danych oraz uniemożliwić nieuprawniony dostęp do danych. Konieczny byłby zewnętrzny audyt sprawdzający właściwe funkcjonowanie systemu i wszystkich jego zabezpieczeń. W systemie należałoby zapisać wszystkie niezbędne procedury dotyczące dostępu do danych osobowych, ich poprawiania, a także odpowiednie procedury odwoławcze.

Podsumowując zgodnie z wnioskiem Parlamentu Europejskiego i Rady, Komisja oceniła możliwe warianty dotyczące systemu TFTS UE, w tym systemu przechowywania i pobierania danych.

Niniejsza ocena uwzględnia zasady zapisane w strategii zarządzania informacjami, która została przyjęta za prezydencji szwedzkiej. Każdy system musi być niezbędny, proporcjonalny i efektywny pod względem kosztów oraz zgodny z prawami podstawowymi. Analiza przeprowadzona przez Komisję, szczegółowo opisana powyżej i w ocenie skutków, pokazuje, że każdy z realnych wariantów ma wady i zalety. Komisja pominęła jednak te warianty, które nie są realne, co wyjaśniono powyżej.

W świetle zebranych informacji argumenty przemawiające za przedstawieniem na tym etapie wniosku dotyczącego systemu TFTS UE nie wydają się wystarczające.

Komisja z zadowoleniem przyjmie opinie Parlamentu Europejskiego i Rady w sprawie tego komunikatu.