PANOPTYKON
FUNDACJA

Zarząd: Katarzyna Szymielewicz, Małgorzata Szumańska
Rada programowa: Adam Bodnar, Ewa Charkiewicz,
Dominika Dörre-Nowak, Joanna Kamiol, Monika Płatek,
Maciej Ślusarek, Piotr Waglowski, Roman Wieruszewski

Pan
Michał Serzycki
Generalny Inspektor
Ochrony Danych Osobowych

Warszawa, 21 czerwca 2010 r.

Szanowny Panie,

W imieniu Fundacji Panoptykon – organizacji działającej na rzecz ochrony praw człowieka wobec zagrożeń związanych z rozwojem społeczeństwa nadzorowanego – chciałabym zainteresować Pana sprawą negocjacji kontrowersyjnego porozumienia o przekazywaniu danych bankowych do Stanów Zjednoczonych za pośrednictwem sieci SWIFT. Poniżej znajdzie Pan krótkie wyjaśnienie politycznego tła sprawy oraz stanowisko Fundacji kwestionujące zgodność negocjowanego porozumienia z przyjętymi przez Polskę standardami ochrony prawa do prywatności oraz ochrony danych osobowych.

SWIFT (Society for Worldwide Interbank Financial Telecomunication), 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, a głównymi uczestnikami większości procesów są kraje europejskie. Działanie na tak dużą skalę musi budzić zainteresowanie obywateli Unii Europejskiej. Jednocześnie, informacje o operacjach bankowych po 11 września 2001 roku stały się obiektem szczególnego zainteresowania ze strony służb specjalnych. Kontrowersje wokół SWIFT pojawiły się po raz pierwszy w 2006 roku, kiedy media ujawniły, że administracja Stanów Zjednoczonych posiada dostęp do danych przechowywanych przez międzynarodowe stowarzyszenie finansowe SWIFT mające swoją siedzibę w Belgii. W lipcu 2009 roku media poinformowały, że w wyniku zmian w strukturze organizacyjnej stowarzyszenia i budowy nowego centrum przechowywania danych w Szwajcarii, konieczne będzie zawarcie nowego porozumienia.

W rezolucji przyjętej we wrześniu 2009 roku posłowie Parlamentu Europejskiego domagali się, aby porozumienie respektowało prawa obywateli Unii Europejskiej do ochrony ich danych osobowych. Podkreślano wtedy, że dane powinny być gromadzone i przetwarzane "wyłącznie w celu zwalczania terroryzmu" oraz domagano się konieczności znalezienia "właściwej równowagi między środkami bezpieczeństwa a ochroną wolności obywatelskich i praw podstawowych". W tym miesiącu Komisja Europejska zaakceptowała nowe porozumienie między Stanami Zjednoczonymi a Unią Europejską, które będzie teraz przedmiotem dyskusji w Parlamencie Europejskim. Fundacja Panoptykon widzi w poszczególnych postanowieniach tego porozumienia, potencjalne niebezpieczeństwa z punktu widzenia ochrony praw człowieka.

W naszej opinii porozumienie SWIFT nie służy zachowaniu właściwej równowagi pomiędzy wartością, jaką jest zapewnienie bezpieczeństwa publicznego, a zagwarantowaniem prawa do prywatności i ochrony danych osobowych. Po pierwsze, porozumienie zakłada przekazywanie amerykańskim służbom hurtowych ilości danych osobowych dotyczących wszystkich klientów banków i instytucji finansowych, bez konieczności wykazywania, że konkretne osoby znajdują się w kręgu podejrzeń o działania związane z finansowaniem terroryzmu, ani też że toczy się w ich sprawie jakiekolwiek postępowanie. W tym sensie postanowienia dotyczące transferu danych naruszają podstawowe zasady prawa do ochrony danych osobowych, czyli zasady niezbędności i proporcjonalności. Tak głębokich naruszeń prawa do prywatności nie będzie można później naprawić przy pomocy mechanizmów nadzoru i kontroli.

Po drugie, porozumienie w obecnym kształcie nie gwarantuje obywatelom Unii Europejskiej, poddanym procedurze przekazywania danych, odpowiednich środków ochrony prawnej. Dane gromadzone w ramach systemu SWIFT powinny podlegać takim samym sądowym procedurom odwoławczym, jakie stosuje się w wypadku danych zbieranych na terenie Unii Europejskiej. Obejmują one między innymi odszkodowania w razie niezgodnego z prawem przetwarzania danych osobowych. Po trzecie, wysuwane są poważne zastrzeżenia co do skuteczności gromadzenia hurtowych ilości danych jako środka przeciwdziałania terroryzmowi. Jak wskazują przeprowadzone badania, dane zaczerpnięte z tego typu źródeł nie są ani niezbędne, ani wystarczające do przeciwdziałania aktom terroryzmu. Wreszcie, kontrowersje i wątpliwości prawne budzi czas, przez jaki dane zgromadzone przez służby specjalne mają być przechowywane. Pięcioletni okres wydaje się nazbyt długi i pozbawiony merytorycznego uzasadnienia. Tak drastyczne jego wydłużenie w odniesieniu do innych środków bezpieczeństwa, np. retencji danych telekomunikacyjnych, gdzie górnym limitem czasu przechowywania danych są dwa lata, wydaje się niewspółmierne do celu zbierania danych.

Władze państwowe obowiązane są do zapewnienia odpowiednich form ochrony praw obywatelskich, takich jak prawo do prywatności i ochrony danych osobowych, nie tylko poprzez wydawanie wewnętrznie obowiązujących aktów normatywnych, ale również monitoring działań podejmowanych na arenie międzynarodowej. Członkostwo Rzeczypospolitej Polskiej w organizacjach o zasięgu europejskim i światowym wymaga stałej czujności w obszarze podejmowanych inicjatyw regulacyjnych i zawieranych porozumień, które mogą mieć zasadniczy wpływ na standard ochrony danych osobowych w Polsce. Wobec powyższego zgodnie z art. 12 ustawy z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (Dz. U. Nr 133, poz. 883 z późn. zm.) prosimy o zbadanie przedmiotowej sprawy i poinformowanie o wynikach przeprowadzonego postępowania.

Z poważaniem,

Katarzyna Szymielewicz

Dyrektorka Fundacji