



Warszawa, 21 czerwca 2010 roku

APEL

O ODRZUCENIE POROZUMIENIA W SPRAWIE SWIFT

W związku z tym, że Komisja Europejska zaakceptowała nowe porozumienie między Stanami Zjednoczonymi a Unią Europejską o przekazywaniu danych bankowych za pośrednictwem sieci SWIFT, wzywamy posłów Parlamentu Europejskiego do ponownego odrzucenia tej umowy ze względu na zagrożenia dla podstawowych praw obywateli Unii Europejskiej, jakie wiązałyby się z jej wejściem w życie. W opinii społeczeństwa obywatelskiego, porozumienie o przekazywaniu danych bankowych SWIFT w przyjętym przez Komisję kształcie jest niezgodne ze standardami obowiązującymi w demokratycznym państwie prawa, w szczególności prawem do prywatności oraz zasadami ochrony danych osobowych, potwierdzonych także w Karcie Praw Podstawowych Unii Europejskiej.

W ramach SWIFT, pośredniczącego 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. Ewentualne wykorzystanie informacji generowanej przez ten system dla celów bezpieczeństwa musi budzić zainteresowanie obywateli Unii Europejskiej, szczególnie jeśli mają być one wykorzystywane przez służby specjalne w państwach trzecich.

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 jakiegokolwiek postępowanie. W tym sensie postanowienia dotyczące transferu danych naruszają podstawowe zasady ochrony danych osobowych, czyli zasadę 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 poddanych 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 badania, dane zaczerpnięte z tego typu źródeł nie są ani niezbędne, ani wystarczające do przeciwdziałania aktom terroryzmu.

Wreszcie, można mieć wątpliwości co do czasu, przez jaki dane mają być przechowywane. Pięcioletni okres wydaje się zbyt długi i pozbawiony merytorycznego uzasadnienia. Tak znaczące wydłużenie terminu – np. w stosunku retencji danych telekomunikacyjnych, gdzie górnym limitem czasu przechowywania danych są dwa lata – jest niewspółmierne do celu zbierania danych.

Z satysfakcją przyjęliśmy rezolucję Parlamentu Europejskiego przyjętą we wrześniu 2009 roku, w której posłowie domagali się, aby porozumienie w sprawie SWIFT respektowało prawa obywateli Unii Europejskiej do ochrony ich danych osobowych, oraz definitywne odrzucenie w lutym 2010 roku pierwszego projektu stałego porozumienia pomiędzy Unią Europejską a Stanami Zjednoczonymi. Podkreślano wtedy, że dane powinny być gromadzone i przetwarzane “wyłącznie w celu zwalczania terroryzmu” i domagano się konieczności znalezienia “właściwej równowagi między środkami bezpieczeństwa a ochroną wolności obywatelskich i praw podstawowych”.

Mamy nadzieję, że i tym razem **posłowie staną na straży wartości istotnych dla Polski i Unii Europejskiej** – jako przestrzeni bezpieczeństwa – przy poszanowaniu wolności i sprawiedliwości.

O FUNDACJI PANOPTYKON

Fundacja Panoptykon działa na rzecz ochrony praw człowieka wobec zagrożeń związanych z rozwojem społeczeństwa nadzorowanego. Analizujemy ryzyka związane wykorzystywaniem nowoczesnych technologii do zwiększenia kontroli nad społeczeństwem, monitorujemy działanie i zmiany prawa, podejmujemy interwencje, informujemy oraz prowokujemy debatę społeczną na temat zagrożeń związanych ze współczesnym nadzorem. Zależy nam na tym, by działania służące zapewnieniu bezpieczeństwa czy sprawnego zarządzania były realizowane z poszanowaniem takich wartości jak wolność i prywatność.