Koniec „Bezpiecznej Przystani”

7 października 2015

Trybunał Sprawiedliwości Unii Europejskiej (TSUE) stwierdził nieważność decyzji Komisji Europejskiej, zgodnie z którą amerykańskie firmy uczestniczące w programie Safe Harbour były uznawane za zapewniające odpowiedni stopień ochrony przekazywanych danych osobowych. Tym samym amerykańskie spółki otrzymujące dane ze Starego Kontynentu będą musiały stosować się do tych samych zasad co firmy operujące w innych krajach poza Unią Europejską. Czy zatem czeka nas zmiana standardu ochrony danych na lepszy? Niekoniecznie. Praktyczna wykładnia wyroku TSUE wobec takich potentatów w eksploatacji danych jak Facebook leży teraz w rękach krajowych organów ochrony danych. Natomiast dużo szybciej i mocniej możemy odczuć jego polityczne skutki, szczególnie w kontekście trwających negocjacji umowy TTIP.

TŁO SPORU

Amerykańskie i europejskie podejście do ochrony danych osobowych różnią się zasadniczo. W USA regulacje prawne w tej sferze są rozproszone i sektorowe, w efekcie wszystko to, co nie jest wprost zakazane, jest dozwolone. Natomiast w UE istnieją ogólne, ponadsektorowe ramy prawne (Dyrektywa 95/46/WE), zgodnie z którymi przetwarzanie danych jest dopuszczalne tylko na podstawie ściśle określonych przesłanek (np. przepisu prawa, wykazania, że jest to konieczne dla realizacji umowy, czy zgody podmiotu danych).

Mimo tego w 2000 roku, po długich i żmudnych negocjacjach z USA, Unia Europejska uznała, że amerykańskie firmy, które przystąpią do programu Safe Harbour („Bezpieczna Przystań”), będą traktowane jako zapewniające odpowiedni poziom ochrony danych osobowych. Firma lub inny podmiot musi jedynie

zadeklarować, że przestrzega określonych zasad i zgłosić się do Departamentu Handlu USA. To, na ile firmy rzeczywiście stosują uzgodnione między USA a UE standardy, jest bardzo rzadko weryfikowane. Przeprowadzone przez Komisję Europejską ewaluacje programu wykazały wręcz, że prawa Europejczyków są notorycznie łamane przez firmy, które przystąpiły do programu. Kolejny problem, na który światło rzuciły dopiero rewelacje Edwarda Snowdena, polega na tym, że „Bezpieczna Przystań" w żaden sposób nie chroni danych Europejczyków przed ich wykorzystaniem przez amerykańskie organy, w tym agencje wywiadowcze.

Program Safe Harbour stanowi zatem poważny wyłom w europejskim systemie ochrony danych, który – co do zasady – nie pozwala na ich przekazywanie poza obszar UE bez odpowiednich gwarancji. Wychodząc z tego założenia, Maximilian Schrems, austriacki prawnik i aktywista, w 2013 zakwestionował legalność transferu swoich danych zamieszczonych na Facebooku na serwery, które ta firma posiada w Stanach Zjednoczonych. Schrems zwrócił się do irlandzkiego organu ochrony danych osobowych (którego jurysdykcji podlega europejski oddział amerykańskiego giganta), by ten wydał decyzję zakazującą Facebookowi takich praktyk. Organ jednak stwierdził, że jest związany wspomnianą decyzją Komisji Europejskiej z 2000 r., i odmówił rozpatrzenia sprawy. Schrems nie poddał się, a sprawa trafiła do irlandzkiego sądu najwyższego, który uznał, że ten spór powinien rozstrzygnąć Trybunał Sprawiedliwości Unii Europejskiej.

CO PRZESĄDZA WYROK TSUE?

Rozpatrywana przez TSUE sprawa formalnie dotyczyła kompetencji organów ochrony danych i tego, czy mogą one kwestionować decyzje Komisji Europejskiej o zapewnianiu przez konkretny kraj lub sektor gospodarki odpowiedniego poziomu ochrony danych. W tym sporze Trybunał jasno opowiedział się po stronie organów ochrony danych i orzekł, że istnienie decyzji Komisji stwierdzającej, że państwo trzecie zapewnia odpowiedni stopień

ochrony przekazywanych danych osobowych, nie ogranicza przysługujących im uprawnień. A zatem, bez względu na ocenę i decyzje Komisji Europejskiej, krajowe organy mają obowiązek kontrolować to, czy zasady, na jakich dane Europejczyków są przekazywane do krajów trzecich – w tym USA – spełniają standardy przewidziane w Dyrektywie i Karcie praw podstawowych UE. W tym zakresie wyrok wzmacnia pozycję takich organów jak polski GIODO i wręcz nakazuje im weryfikować, czy zagraniczne firmy podlegające ich jurysdykcji działają zgodnie z prawem UE.

Na tym jednak treść wyroku się nie kończy. Trybunał poszedł krok dalej, niż sugerowałoby pytanie zadane przez irlandzki sąd, i ocenił, na ile reguły ochrony danych przewidziane w programie Safe Harbour (stanowiące podstawę decyzji Komisji Europejskiej z 2000 r.), są zgodne ze standardami, jakie wynikają z Dyrektywy 95/46/WE i Karty praw podstawowych. W tym zakresie doszedł do wniosku, że nie są – przede wszystkim dlatego, że prawo amerykańskie pozwala organom publicznym na niemal nieograniczony i niekontrolowany dostęp do danych Europejczyków, a tym samym podważa istotę prawa do prywatności. Ten element wyroku jest niezwykle ważny, ponieważ przesądza, że dopóki Amerykanie nie zmienią swojego prawa w zakresie, w jakim pozwala ono na masową inwigilację, dopóty – z perspektywy Unii Europejskiej – ich standardy ochrony danych będą uznawane za niewystarczające. Zdaniem Trybunału w amerykańskim systemie prawnym brakuje też realnych gwarancji proceduralnych dla Europejczyków, w tym prawa do sądu i konkretnych uprawnień związanych z ochroną danych osobowych (np. do udostępnienia i korekty danych).

PRAKTYCZNE SKUTKI W RĘKACH KRAJOWYCH ORGANÓW

W praktyce wyrok TSUE otwiera krajowym organom ochrony danych drogę do postępowań kontrolnych, które mogą się zakończyć uznaniem, że dane z konkretnych europejskich spółek – np. irlandzkiego oddziału Facebooka – nie mogą być przekazywane do USA. Biorąc jednak pod uwagę, jak elastyczne i łagodne reguły

transferu danych przewiduje obecnie obowiązująca Dyrektywa, tak radykalny skutek wydaje się mało prawdopodobny. Przede wszystkim transfer danych nadal będzie możliwy w oparciu o tak szerokie i stosunkowo łatwe do wykazania przesłanki, jak konieczność przekazywania danych dla realizacji umowy, wymóg wynikający z prawa czy zgoda osoby, której dane dotyczą. Co więcej: nawet w przypadku braku takich podstaw firmy, które chcą lub muszą przekazywać dane do USA, będą mogły wystąpić o indywidualną zgodę GIODO lub jego odpowiednika w innym kraju UE. Aby taką zgodę uzyskać, firma powinna wykazać, że zapewniła odpowiednie zabezpieczenia w zakresie ochrony prywatności.

Organy ochrony danych będą zatem oceniać sytuację konkretnych firm oraz proponowane przez nie standardy i zabezpieczenia, a nie ogólne reguły obowiązujące w Stanach Zjednoczonych. Zgodnie z dyrektywą firma może zapewnić odpowiedni poziom ochrony przekazywanych danych osobowych np. poprzez przyjęcie odpowiednich zobowiązań umownych, takich jak wzorcowe klauzule (zaakceptowane przez Komisję Europejską) czy wiążące reguły korporacyjne.

Trudno przewidzieć, czy taki standard wystarczy poszczególnym krajowym organom i jakie decyzje ostatecznie podejmą, szczególnie w kontekście uznania przez TSUE, że amerykańskie prawo – w zakresie, w jakim umożliwia masową inwigilację Europejczyków – jest nie do pogodzenia z europejskimi standardami. Faktem jest, że żadne zobowiązania umowne nie ochronią klientów amerykańskich firm przed takim zagrożeniem. Obserwując dotychczasowe perypetie Schremsa w walce z Facebookiem i ewidentną opieszałość irlandzkiego organu, który w tej sprawie nie podjął żadnej wiążącej decyzji, można się spodziewać, że przynajmniej niektóre organy, mimo prawnych wątpliwości, wydadzą decyzje pozwalające na przekazywanie danych do USA. Jeśli tak się stanie, praktyczne skutki wyroku TSUE będą miały raczej wymiar proceduralny – zmienią się podstawy przekazywania danych, ale nie zmieni się standard ich

ochrony.

WYMIAR POLITYCZNY

Trudno natomiast nie docenić skutków wyroku TSUE na poziomie politycznym. Można go potraktować jako zapowiedź politycznych i prawnych obstrukcji w przekazywaniu danych, jeśli Amerykanie nie zdecydują się na wzmocnienie standardów ich ochrony, przynajmniej w sferze ich udostępniania organom publicznym.

Będzie to miało znaczenie nie tylko dla trwających prac nad rozporządzeniem dotyczącym ochrony danych osobowych, które ma obowiązywać również firmy amerykańskie, ale przede wszystkim dla negocjacji umowy TTIP. To szerokie porozumienie, przewidujące ujednolicenie standardów regulacyjnych, siłą rzeczy będzie dotyczyło również transferów danych. W świecie usług opartych o eksploatację danych trudno sobie wyobrazić ich swobodny przepływ i realne otwarcie obu rynków dla firm z jakiejkolwiek branży bez ujednolicenia reguł ochrony prywatności. Wobec unieważnienia decyzji Komisji Europejskiej, która dotychczas umożliwiała swobodny transfer danych na linii UE–USA, rozwiązanie tego problemu zyskuje jeszcze wyższy polityczny priorytet. A więc należy się spodziewać, że temat transferów danych będzie przedmiotem dyskusji w kolejnej rundzie. Wyrok TSUE daje Komisji Europejskiej przynajmniej argument do twardych negocjacji.

Autorstwo: Katarzyna Szymielewicz
Współpraca merytoryczna: Jędrzej Niklas
Źródło: Panoptykon.org

BIBLIOGRAFIA

1. http://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117pl.pdf

2. http://eur-lex.europa.eu/legal-content/pl/ALL/?uri=CELEX:32000

D0520

3. http://www.bna.com/eu-cites-us-n17179891134/

4. http://www.reuters.com/article/2014/06/18/us-facebook-privacy-idUSKBN0ET11X20140618