Odlotowa inwigilacja ochroni nas przed terroryzmem?

15 kwietnia 2016

Obywatele mają zyskać większą kontrolę nad swoimi danymi, a firmy mają skorzystać z jednolitych zasad ochrony danych w całej UE. Parlament Europejski przyjął nowe unijne przepisy w zakresie ochrony danych.

Parlament Europejski przyjął nowe unijne przepisy dotyczące ochrony danych. Prace nad nimi nazywano Wielką Reformą Prywatności. Trwały one od roku 2013 i teraz trochę trudno uwierzyć, że wreszcie udało się doprowadzić sprawę do końca.

Nowe przepisy w zakresie ochrony danych mają zastąpić dyrektywę z 1995 roku. Z tego powodu wiele osób mówi, że nowe przepisy dostosowują ochronę danych w UE do „epoki cyfrowej".

„Rozporządzenie dotyczące ochrony danych sprawi, że wysoki, ujednolicony poziom ochrony danych w całej Unii Europejskiej stanie się rzeczywistością. To wielki sukces dla Parlamentu Europejskiego i zdecydowane europejskie „tak" dla silnej ochrony praw konsumentów i konkurencji w epoce cyfrowej" – mówił poseł-sprawozdawca Jan Philipp Albrecht.

Przypomnijmy krótko o co chodzi w tej „Wielkiej Reformie". Składa się ona z dwóch elementów -rozporządzenia oraz dyrektywy. Rozporządzenie ma ułatwić obywatelom kontrolowanie swoich danych. Dyrektywa odnosi się do działań organów ścigania.

Reforma ma zagwarantować m.in. łatwiejszy dostęp do własnych danych. Ma też ułatwić przenoszenie danych pomiędzy różnymi dostawcami usług.

Nowe przepisy precyzują tzw. prawo do bycia zapomnianym. Poza tym obywatele powinni wiedzieć kiedy dojdzie do wycieku

danych, gdyż firmy i organizacje będą musiały powiadamiać władze o „poważnych wyciekach” (w toku prac nad reformą dyskutowano m.in. o tym jak poważny musi być wyciek, aby trzeba było o nim informować).

Reforma ma również wprowadzić surowsze kary dla firm za naruszenia prawa ochrony danych. Obecnie te kary mają znaczenie raczej symboliczne, czego przykładem może być ukaranie firmy Google karą w wysokości 150 tys. euro. Teraz firmom takim jak Google będzie groziła kara do 4% rocznego obrotu. To już może zaboleć.

Ponadto z punktu widzenia firm istotne będzie ustanowienie jednolitego systemu zasad dla całej unii oraz mechanizmu one-stop-shop. Chodzi o to, że przedsiębiorca rozlicza się ze swoich obowiązków w jednym miejscu, a nie przed wszystkimi organami ochrony danych osobowych we wszystkich krajach UE.

Jak już wspomniano, pakiet legislacyjny ochrony danych obejmuje też dyrektywę w sprawie przekazywania danych do celów policyjnych i sądowych. Ma ona zastosowanie do ponadgranicznego przekazywania danych na terytorium UE, a także określa minimalne standardy dotyczące przetwarzania danych dla potrzeb policji we wszystkich państwach członkowskich.

„Głównym problemem, jeśli chodzi o ataki terrorystyczne i inne formy przestępczości międzynarodowej, jest niechęć organów ścigania państw członkowskich do wymiany cennych informacji” – mówiła Marju Lauristin, posłanka-sprawozdawczyni prowadząca prace nad dyrektywą. „Poprzez ustanowienie europejskich standardów wymiany informacji między organami ścigania, dyrektywa o ochronie danych stanie się potężnym narzędziem, które pomoże władzom krajowym w łatwym i skutecznym przekazywaniu danych osobowych, przy jednoczesnym poszanowaniu podstawowego prawa do prywatności.”

Co sądzą o przepisach nie-politycy? Pierwotnie zaproponowana

„reforma prywatności” wydawała się o wiele bardziej ambitna niż to, co powstało ostatecznie. Z drugiej jednak strony udało się obronić pewne ważne kwestie, w czym niewątpliwie było trochę zasług Edwarda Snowdena, który wstrząsnął naszym myśleniem o prywatności.

Fundacja Panoptykon – polska organizacja pozarządowa – określiła nowe przepisy jako „kompromis znośny dla biznesu i obiecujący dla obywateli”. Zwracała ona również uwagę na niedoróbki dotyczące m.in. zasad profilowania. Czas pokaże jak nowe przepisy sprawdzą się w rzeczywistości.

Rozporządzenie wejdzie w życie 20 dni po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej. Jego postanowienia będą stosowane bezpośrednio we wszystkich państwach członkowskich dwa lata po tej dacie. Jeśli chodzi o dyrektywę to państwa członkowskie będą miały dwa lata na wdrożenie jej do przepisów krajowych.

Parlament Europejski głosował wczoraj także nad drugą sprawą ważną dla ochrony danych.

Dane pasażerów linii lotniczych będą trafiać do specjalnych jednostek, które będą utworzone na mocy dyrektywy przyjętej dziś przez Parlament Europejski. Powstaną nowe bazy z danymi obywateli, to pewne. Czy w zamian za to będziemy bezpieczniejsi?

Parlament Europejski przyjął dyrektywę w sprawie zarządzania danymi pasażerów linii lotniczych (tzw. dyrektywa PNR). Dziennik Internautów pisał już o tym jak ma działać europejski system PNR. Linie lotnicze mają przekazywać dane pasażerów do specjalnych jednostek, które z kolei będą udostępniały dane służbom.

Za dyrektywą głosowało 461 posłów. Przeciwko było 179, a 9 wstrzymało się od głosu.

Państwa członkowskie będą musiały ustanowić „jednostki do

spraw informacji o pasażerach” (tzw. „JIP”). Informacje będą musiały być przechowywane przez okres pięciu lat, ale po sześciu miesiącach będą „anonimizowane”.

Każda JIP będzie odpowiedzialna za gromadzenie, przechowywanie i przetwarzanie danych PNR, za przekazywanie ich do właściwych organów oraz wymianę ich z jednostkami innych państw członkowskich i Europolem. Teoretycznie każde przekazanie danych ma się odbywać na podstawie oceny indywidualnego przypadku i wyłącznie w celu zapobiegania przestępstwom terrorystycznym lub poważnej przestępczości.

Dyrektywa będzie miała zastosowanie do lotów poza Unię, jednak poszczególne państwa członkowskie będą mogły zdecydować o stosowaniu jej do lotów pomiędzy kajami UE. Państwa członkowskie mogą również zdecydować się na zbieranie i przetwarzanie danych PNR przekazywanych przez biura podróży i organizatorów wycieczek świadczący usługi takie jak rezerwacja lotów.

W celu zapewnienia ochrony danych JIP mają powoływać inspektora ochrony danych, który będzie monitorował sposób przetwarzania danych. Po wstępnym okresie przechowywania dostęp do pełnego zestawu danych PNR, które pozwalają na natychmiastową identyfikację osoby, powinien być możliwy jedynie w ściśle określonych przypadkach i po spełnieniu konkretnych warunków zdefiniowanych w dyrektywie. Wszystkie przypadki przetwarzania danych PNR powinny być zewidencjonowane i udokumentowane.

Zakazane będzie przetwarzanie danych PNR ujawniających rasę lub pochodzenie etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, stan zdrowia, życie seksualne lub orientację seksualną danej osoby (choć szczerze powiedziawszy niektóre z tych rzeczy można wywnioskować z innych danych, mniej lub bardziej skutecznie).

Ustalono, że Komisja Europejska będzie musiała przeprowadzić przegląd dyrektywy dotyczącej unijnego PNR dwa lata po jej wdrożeniu do prawa krajowego. Ta rewizja ma służyć zwłaszcza sprawdzeniu zgodności przetwarzania danych z przyjętymi standardami i w odniesieniu do celów określonych w dyrektywie.

Parlament Europejski jak zwykle jest dumny z kolejnej dyrektywy, ale nie wszyscy się cieszą. Organizacje broniące prywatności od dawna mówiły, że wprowadzenie dyrektywy PNR odbywa się bez należytej dyskusji. Tak naprawdę nie udowodniono, że przetwarzanie danych pasażerów zapobiegnie atakom terrorystycznym. Nie jest też tajemnicą, że ostatnie ataki w Brukseli i w Paryżu stworzyły odpowiedni „klimat emocjonalny" do wprowadzania takich rozwiązań.

Organizacja European Digital Rights (EDRi) nazywała dyrektywę PNR „hańbą". Wskazywała na to, że nie powinno się tworzyć kolejnych ogromnych baz danych dotyczących niewinnych obywateli. Na ten sam problem zwracała uwagę polska Fundacja Panoptykon.

„Europejski System PNR opiera się na założeniu, że każdy podróżny to potencjalny terrorysta lub inny groźny przestępca. W praktyce uderzy jednak przede wszystkim w osoby podróżujące z „podejrzanych" krajów. Może to prowadzić w praktyce do dyskryminacji i utrwalania krzywdzących stereotypów, mimo że same przepisy bezpośrednio dyskryminacji zakazują. Co więcej, raz zebrane dane zaczynają żyć własnym życiem – trudno dziś przewidzieć, do jakich celów decydenci polityczni czy same służby zechcą je wykorzystać w przyszłości" – czytamy na stronie Fundacji.

Projekt musi być jeszcze formalnie zatwierdzony przez Radę. Po opublikowaniu w Dzienniku Urzędowym Unii Europejskiej, państwa członkowskie będą miały dwa lata na wdrożenie zapisów dyrektywy do prawa krajowego.

Autorstwo: Marcin Maj

Źródło: DI.com.pl
Kompilacja 2 wiadomości: WolneMedia.net