Unijny projekt o ochronie prywatności w Internecie

20 stycznia 2017

Komisja Europejska zaprezentowała projekt rozporządzenia, które reguluje ochronę prywatności użytkowników Internetu. Nowymi regułami zostaną objęte nie tylko tradycyjne firmy telekomunikacyjne, ale również WhatsApp, Skype czy Viber.

Zmienione zasady mają wzmocnić ochronę danych oraz poufność komunikacji elektronicznej. Zastąpią obowiązującą od 2002 roku dyrektywę dotyczącą e-prywatności (była wcześniej rewidowana tylko raz, w 2009 roku). Od czasu jej przyjęcia krajobraz usług komunikacyjnych znacznie się zmienił. Na rynek weszły podmioty, które wymykają się obecnym przepisom. Firmy zaś stosują coraz bardziej wyszukane metody śledzenia użytkowników oraz analizowania ich danych. Projekt Komisji Europejskiej (KE) ma to zmieniać i dostosować prawo do dynamicznie przeobrażającej się rzeczywistości. Jeżeli unijni decydenci oprą się agresywnemu lobbingowi biznesu – czekają nas lepsze reguły ochrony prywatności w Internecie.

Projekt rozporządzenia został przekazany do dalszych prac w Parlamencie Europejskim. Swoje stanowiska wypracowują również kraje członkowskie – w tym polskie Ministerstwo Cyfryzacji. Na potrzeby konsultacji społecznych Fundacja Panoptykon przedstawiła swoje stanowisko w tej sprawie. Podsumowujemy je poniżej i wskazujemy na najważniejsze zmiany w nowym rozporządzeniu.

Co zmienia nowy projekt?

Wspólny standard we wszystkich krajach. KE proponuje, by nowe zasady prywatności użytkowników znalazły się w rozporządzeniu, a w nie dyrektywie jak poprzednio. Nowe prawo będzie więc obowiązywało bezpośrednio we wszystkich krajach Unii, a państwa nie będą musiały wprowadzać dodatkowych ustaw

krajowych. Dzięki temu zwiększa się szansa na spójne wdrożenie przepisów i lepszą ochronę użytkowników. Rozporządzenie ustanawia też obowiązki nie tylko dla firm europejskich, ale dla wszystkich podmiotów adresujących swoje usługi do Europejczyków.

Rozszerzony zakres. Dyrektywą objętą były do tej pory tradycyjne firmy telekomunikacyjne. Nowe rozporządzenia będzie obowiązywało również firmy oferujące usługi OTT (over-the-top) – czyli Facebook, WhatsApp, Viber czy Skype. Do nowych reguł będą musieli się dostosować również dostawcy takich usług, dla których komunikacja między użytkownikami jest jedynie dodatkiem (dotyczy to np. gier z opcją komunikatora). To dobre rozwiązanie, które gwarantuje, że nowe przepisy będą obowiązywały wszędzie tam, gdzie użytkownicy faktycznie się komunikują za pomocą narzędzi elektronicznych. Ten nowy język przepisów być może będzie bardziej „odporny" na zmiany technologiczne niż obecne rozwiązania.

Nowe rodzaje danych. Projekt rozporządzenia wprowadza dwa rodzaje danych dotyczących użytkowników – dane dotyczące treści i tzw. metadane (czyli np. informacje o lokalizacji konkretnego urządzenia). Dzięki temu być może uniknie się problemów interpretacyjnych wywołanych przez obecną dyrektywę, która mówi o dodatkowym podziale na dane lokalizacyjne i dane o ruchu. Mogą jednak pojawić się wątpliwości, czy konkretna informacja jest treścią, czy metadaną (jak np. w przypadku adresu URL). Te niejasności trzeba by wyjaśnić w trakcie dalszych prac nad projektem. KE chce ustanowić też różne zasady przetwarzania dla treści i metadanych. O ile pewne różnice są zrozumiałe, to warto zastanowić się, czy projekt nie wprowadza zbyt wielu komplikacji. Szczególne kontrowersje wiążą się również ze zgodą jako podstawą do analizowania treści naszej komunikacji – czyli np. skanowania e-maili.

Poufność komunikacji, również między urządzeniami. Projekt Komisji Europejskiej zakazuje – co do zasady – podsłuchiwania, monitorowania i nadzorowania naszej komunikacji. Przetwarzanie

danych będzie możliwie tylko w określonych sytuacjach (np. dla zapewnienia bezpieczeństwa komunikacji) lub za zgodą użytkownika. Nowymi regułami objęte będą jednak nie tylko komunikaty, które aktywnie i świadomie wysyłają użytkownicy. Projekt ustala również zasady w sytuacji, gdy informacje przesyłają same urządzenia. Dzięki temu ochrona prywatności będzie dotyczyła również obszaru tzw. Internetu rzeczy – czyli tych różnych urządzeń gospodarstwa domowego czy tzw. wearables, które mogą ujawniać np. dane o stanie zdrowia czy przyzwyczajaniach żywieniowych.

Zakaz śledzenia i ustawienia prywatności. Firmy nie będą mogły instalować na urządzeniach użytkowników bez ich zgody ciasteczek oraz innych narzędzi umożliwiających śledzenie ich aktywności. Wyjątkiem od tej zasady będą m.in. ciasteczka analityczne, umożliwiające liczenie odwiedzin na konkretnej stronie. Zgodę będzie można wyrazić poprzez ogólne ustawienia prywatności wyszukiwarek. Dzięki takiej praktyce Komisja Europejska chce ułatwić korzystanie z Internetu i ograniczyć wyskakujące permanentnie okna, proszące o zgodę na ciasteczka. To dobre rozwiązanie, które jednak zatrzymuje się w pół drogi. Przede wszystkim nie tylko wyszukiwarki, ale również ogólne ustawienia np. smartfona powinny pozwalać na ustawienia prywatności przy ściąganiu aplikacji. Co więcej, ustawienia prywatności w opcji domyślnej powinny gwarantować najwyższy możliwy poziom ochrony danych użytkowników i m.in. zakazywać ich śledzenia. Dopiero udzielona przez użytkowników wyraźna zgoda mogłaby zezwalać firmom na takie praktyki.

Wysokie kary i nadzór GIODO. Tak jak w przypadku ogólnego rozporządzenia o ochronie danych osobowych (RODO) odpowiedzialnym za nadzór nad nowymi przepisami będzie organ ochrony danych osobowych – w Polsce będzie to Generalny Inspektor Ochrony Danych Osobowych (GIODO). Dzięki temu wszystkie kwestie związane z ochroną danych znajdą się „pod jednym dachem”. To GIODO będzie rozpatrywał skargi i badał naruszenia nowych reguł. Za ich złamanie będą grozić wysokie i

realne kary, nawet od 2% do 4% globalnego obrotu danej firmy.

Organizacje społeczne nie będą mogły bronić użytkowników. Projekt rozporządzenia pozwala użytkownikom na składanie skarg na naruszenia ich praw do organu ochrony danych, a nawet żądać odszkodowania. Niestety KE nie przewidziała możliwości, by organizacje społeczne mogły reprezentować osoby indywidualne w takich sprawach. Tego typu rozwiązanie jest obecne w RODO oraz w prawie konsumenckim. Tymczasem udział organizacji non profit, posiadających wyspecjalizowaną wiedzę i doświadczenie, może wzmocnić pozycję i ochronę użytkowników. Dotyczy to zwłaszcza tych spraw, gdy po drugiej stronie są duże międzynarodowe korporacje.

Dostęp służb do danych Internautów. Nowy projekt pozwala na tworzenie krajowych przepisów umożliwiających sięganie służb oraz organów administracji po dane Internautów. Wyjątki takie będą możliwe jednak, gdy okaże się to niezbędne do walki z terroryzmem czy przestępczością. Jednocześnie firmy będą musiały ustanowić wewnętrzne zasady udostępniania danych organom publicznym. Na żądanie GIODO usługodawcy będą musieli przekazać informacje o tym, jaki podmiot publiczny i w jakich sprawach wnioskował o dane użytkowników. Nowe przepisy gwarantują więc pewien stopień przejrzystości, są jednak niewystarczające. Naszym zdaniem firmy powinny zostać zobowiązane do cyklicznego przekazywania do organu ochrony danych statystyk wskazujących, kto pytał i po co o dane użytkowników. GIODO powinien wówczas podawać te zbiorcze informacje do opinii publicznej.

KE chce, by projekt został przyjęty tak, by mógł zacząć obowiązywać w maju 2018 roku – tak samo jak RODO. To dobry pomysł, dzięki któremu można by uniknąć pewnego zamętu we wprowadzaniu nowych przepisów. Jednak wydaje się, że takie plany mogą okazać się nierealistyczne. Dla porównania: prace nad RODO trwały znacznie dłużej, niż przewidywano na początku. Sytuacji zapewne nie ułatwi intensywny lobbing ze strony sektora biznesu, którego w przypadku tego projektu należy się

spodziewać. Zapewne czekać nas będzie kolejna długa i wytężona debata polityczna, w której stawką będzie lepsza ochrona prywatności i poufności użytkowników Internetu.

Autorstwo: Jędrzej Niklas
Źródło: Panoptykon.org