

FBI CHCE DOSTĘPU DO DANYCH FACEBOOKA. PRYWATNOŚĆ WAŻNIEJSZA OD BEZPIECZEŃSTWA?

Jak informuje dziennik "The Wall Street Journal", plany amerykańskiego Federalnego Biura Śledczego, odnoszące się do gromadzenia danych na masową skalę z portalu Facebook, mogą naruszać zasady polityki prywatności platformy. Według FBI dostęp do tych informacji jest potrzebny, aby skutecznie walczyć z przestępczością.

Nowojorska gazeta donosi, że FBI rozważa obecnie masowe gromadzenie danych z Facebooka, Twittera i innych sieci społecznościowych celem "proaktywnego identyfikowania i reaktywnego monitorowania zagrożeń wobec USA i interesów kraju". Ogłoszenie o przetargu dla firm, które miałyby współpracować przy tym projekcie z instytucją, zostało opublikowane w ubiegłym miesiącu, kilka tygodni przed zamachami z Ohio i Teksasu, po których prezydent USA Donald Trump wezwał platformy internetowe do aktywnego wykrywania możliwych zamachowców. Termin zgłaszania propozycji upływa 27 sierpnia - informuje "The Wall Street Journal".

Program, który chce realizować FBI, może jednak stać w sprzeczności z regulaminem Facebooka, zabraniającym wykorzystywania danych tam zgromadzonych na potrzeby nadzoru elektronicznego. Federalne Biuro Śledcze odmówiło "WSJ" komentarza w związku ze sprawą. Podkreśliło jednak, że wewnątrz instytucji panuje przekonanie, iż dane "mogą być zbierane z zachowaniem wszystkich wolności obywatelskich i z poszanowaniem prywatności".

Przedstawicielka Twittera odnosząc się do sprawy stwierdziła, iż polityka firmy również - podobnie jak w przypadku Facebooka - zabrania wykorzystywania danych "przez jakikolwiek podmiot do celów nadzoru elektronicznego bądź w jakikolwiek inny sposób, który stałby w sprzeczności z oczekiwaniami naszych użytkowników odnośnie prywatności".

Według "WSJ" projekt FBI dotyczy danych dostępnych publicznie, nie zaś tych, które w mediach społecznościowych użytkownicy zamieszczają stosując ograniczenia widoczności wynikające z ustawień prywatności, w tym prywatnych wiadomości. Informacje, które miałyby być gromadzone w ramach programu to imiona i nazwiska użytkowników, ich indywidualne numery identyfikacyjne oraz zdjęcia. Według ekspertów cytowanych przez "WSJ" dane te jednak w zestawieniu z informacjami z innych źródeł mogą być wykorzystane przez służby do budowy zaawansowanych profili użytkowników oraz monitorowania ich codziennego życia.

Jednocześnie, jak zaznacza dziennik, FBI wraz z innymi ścigania znajdują się pod rosnącą presją wynikającą z coraz większych wyzwań, wobec przemocy i przypadków terroryzmu wewnątrz kraju. Wiele ostatnich aktów terroru zostało dokonanych przez mężczyzn, którzy dyskutowali na temat swoich nienawistnych ideologii na forach internetowych i w mediach społecznościowych, w niektórych przypadkach dając sygnały ostrzegawcze wiele miesięcy wcześniej, nim zaatakowali - podkreśla gazeta.

Facebook natomiast poddawany jest coraz potężniejszym naciskom, by lepiej chronić dane użytkowników po serii skandali związanych z niewłaściwymi praktykami tej firmy dotyczącymi prywatności - zauważa "WSJ". Koncern Marka Zuckerberga współpracuje rutynowo z organami ścigania w zakresie udostępniania informacji na potrzeby prowadzonych śledztw, przypadków molestowania i przemocy wobec dzieci oraz prób samobójczych, a także innych zagrożeń o znaczącym oddziaływaniu publicznym - przypomina dziennik.

Według "WSJ" sprawa nieautoryzowanego dostępu do danych z platformy i prowadzenia z ich pomocą działań z zakresu nadzoru elektronicznego może być dla Facebooka szczególnie istotna ze względu na zawartą niedawno z Federalną Komisją Handlu ugodę w sprawie związanej z nadużyciami wobec prywatności użytkowników. Ugoda narzuca Facebookowi obowiązek wdrożenia "złożonego programu bezpieczeństwa danych", w tym - właściwego poziomu ochrony danych przed możliwym nieprawidłowym wykorzystaniem.

Przedstawiciel Federalnej Komisji Handlu cytowany przez "WSJ" ocenił, że obowiązujące w USA prawo nakazuje Facebookowi ochronę danych użytkowników przed nieuprawnionym i niepoprzedzonym zgodą gromadzeniem w sposób opisany przez FBI. Jak dodał, obowiązek ten dotyczy nie tylko danych, których widoczność jest ograniczona z użyciem ustawień prywatności, ale też tych informacji, które są publicznie dostępne.

SZP/PAP