Dane 2,4 mln osób z całego świata, w tym Polaków, zgromadziła chińska firma lojalna wobec Komunistycznej Partii Chin



W połowie września 2020 roku wyciekły informacje o tym, że chińska firma Shenzhen Zhenhua Data Technology, powiązana z tajnym oddziałem wojskowym i wywiadowczym Pekinu, zgromadziła gigantyczną bazę danych z plikami dotyczącymi 2,4 mln ludzi z całego świata, w tym dane wpływowych osób i ich rodzin. W ostatnich dniach pojawiły się doniesienia, że ChRL zebrała również dane Polaków.

„Kolekcja" danych z całego globu w komunistycznych rękach

Zhenhua Data Technology, która jest powiązana z Armią Ludowo-Wyzwoleńczą, Ministerstwem Bezpieczeństwa Państwa oraz Komunistyczną Partią Chin (KPCh), zgromadziła bazę skompilowaną głównie z tzw. materiałów open source, takich jak posty w mediach społecznościowych i dane online.

Baza danych okazała się uszkodzona. Australijska firma Internet 2.0, która zajmuje się cyberbezpieczeństwem, odzyskała ponad 10 proc. danych, które były w niej zawarte. Firma ujawniła, że pośród zrekonstruowanych plików znalazły się dane około 52 tys. Amerykanów, 35 tys. Australijczyków, 9

tys. 700 Brytyjczyków i 5 tys. Kanadyjczyków.

W ostatnim tygodniu października „Gazeta Polska” poinformowała w artykule, że otrzymała od Internet 2.0 fragment bazy danych z nazwiskami Polaków. „To spis ponad 3 tys. rekordów zawierających imiona i nazwiska (część się powtarza). Nie wiadomo jednak, z jakiego powodu chiński wywiad wojskowy zlecił Zhenhua zbieranie informacji o tych osobach. Pewne jest jednak, że służba ta ma bardzo dobrą orientację w polskim świecie politycznym. Na liście znajdują się nie tylko byli lub obecni wysocy rangą urzędnicy państwowi, lecz także ich rodziny – małżonkowie, dzieci, rodzice i rodzeństwo” – podaje gazeta.

Internet 2.0 odtworzył zaledwie 10 proc. całej bazy, wydaje się więc, że w tym momencie nie można stwierdzić, czy wśród odzyskanych rekordów znalazły się wszystkie dane Polaków, które zostały zgromadzone w bazie.

Na kogo „poluje” KPCh na całym świecie?

Zgodnie z raportami globalnego konsorcjum medialnego baza danych obejmuje osoby z różnych sektorów – polityki, biznesu, prawa, środowiska akademickiego i obronności – oraz zawiera szczegółowe dane, takie jak daty urodzenia, adresy, stan cywilny i upodobania polityczne.

Znajdują się tam dane dotyczące zarówno zwykłych biznesmenów, jak i wysokiej rangi osobistości, takich jak oficerowie marynarki wojennej Stanów Zjednoczonych, obserwatorzy Chin w Waszyngtonie, osoby ze środowiska naukowego, członkowie brytyjskiej rodziny królewskiej oraz liderzy przedsiębiorczości.

Ta baza danych, nazywana Overseas Key Information Database (OKIDB), pozwala na dostęp do zagranicznych danych politycznych, wojskowych i biznesowych. Zawiera szczegółowe informacje na temat infrastruktury państw, przemieszczania się zasobów wojskowych, a także analizy opinii publicznej.

Mimo że obecnie nie ma dowodów na to, że reżimowe władze wykorzystują oprogramowanie OKIDB, to jak podkreśla „Washington Post", z dokumentów marketingowych i rekrutacyjnych Zhenhua można wnioskować, że jest to „firma patriotyczna", której głównym klientem docelowym jest wojsko.

„The Globe and Mail" po analizie danych dotyczących Kanadyjczyków napisał, że twórcy bazy przypisali osobom z listy „ocenę" w skali od 1 do 3 .

„Wydaje się, że ci, którym przypisano 1, to osoby o bezpośrednim wpływie, takie jak burmistrzowie, posłowie lub wyżsi urzędnicy państwowi, podczas gdy ci, którym przypisano 2, byli często krewnymi osób u władzy […]" – podaje gazeta. Z kolei ci, których oznaczono numerem 3, to najczęściej osoby skazane, przeważnie za przestępstwa gospodarcze – napisał dziennik.

Tajemnicza baza ujrzała światło dzienne

Baza danych została ujawniona przez źródło w Chinach, a informację przekazano profesorowi Christopherowi Baldingowi. To amerykański naukowiec, który do 2018 roku pracował na Uniwersytecie w Pekinie, skąd udało mu się wyjechać ze względów bezpieczeństwa. To dzięki niemu sprawą zajęła się firma Internet 2.0.

14 września Balding opublikował na swojej stronie oświadczenie, w którym napisał, że zajmował się badaniami doniesień dotyczących Huawei. Trwało to do momentu, zanim w jego badaniach nie nastąpił nagły zwrot. Natknął się na „coś, co dla badaczy Chin jest czymś podobnym do odkrycia Świętego Graala" – otrzymał informację o istnieniu tej potężnej bazy danych.

Przekazał ją konsorcjum mediów w Australii, Stanach Zjednoczonych, Kanadzie, Wielkiej Brytanii, Włoszech i Niemczech.

Balding uważa, że dane potwierdzają utrzymywane od dawna podejrzenia, dotyczące działalności KPCh w zakresie nadzoru i monitorowania. „To, czego nie można lekceważyć, to rozległość i szczegółowość nadzoru [prowadzonego przez] chińskie państwo oraz jego zasięg na całym świecie" – podkreśla.

Jak zauważa: „Świat jest dopiero na początkowych etapach zrozumienia, ile Chiny inwestują w wywiad i jak wpływają na operacje, korzystając z surowych danych, musimy zrozumieć ich cele".

We wcześniejszym wpisie naukowiec zwraca uwagę, że KPCh stanowi „bezprecedensowe wyzwanie dla otwartych, kochających wolność państw prawa na całym świecie". Reżim „buduje opresyjne państwo z nadzorem technologicznym, które daje partii komunistycznej potężne środki do kontroli obywateli w kraju" – wyjaśnia.

„Mamy teraz dowody na to, jak chińskie firmy współpracują z agencjami państwowymi w celu monitorowania osób i instytucji na całym świecie" – ocenia Balding.

Reakcja Zhenhua nie zdziwiła ekspertów

Poproszona przez „The Guardian" o komentarz firma Zhenhua zaprzeczyła istnieniu takiej bazy danych, podając, że wszelkie zebrane informacje są danymi ogólnodostępnymi w internecie. Przedstawicielka firmy stwierdziła, że nie zbierają danych i jest to tylko „integracja danych". Zaznaczyła, że model biznesowy i partnerzy stanowią tajemnicę handlową firmy.

Zanegowała również doniesienia, że Zhenhua ma jakiekolwiek powiązania z chińskimi władzami lub wojskiem, dodając, że ich klientami są organizacje badawcze i grupy biznesowe.

W rozmowie z anglojęzyczną edycją „The Epoch Times" eksperci przyznali, że nie byli zaskoczeni takim stanowiskiem chińskiej firmy.

Według Michaela Shoebridge'a, dyrektora programu obrony, strategii i bezpieczeństwa narodowego w think tanku Australian Strategic Policy Institute (ASPI), stwierdzenie Zhenhua „nie może być przyjmowane za dobrą monetę", wziąwszy pod uwagę, że tamtejsze prawo zobowiązuje firmy do pomocy chińskim agencjom bezpieczeństwa i wywiadu. Dodaje, że firmy oczywiście muszą publicznie temu zaprzeczać.

W ocenie Caseya Fleminga, dyrektora generalnego firmy BLACKOPS Partners, zajmującej się strategią wywiadowczą i bezpieczeństwa, zgromadzone w bazie informacje są wykorzystywane do wspierania operacji „nieograniczonej wojny hybrydowej" chińskiego reżimu. Obejmuje to szpiegostwo, tajne zagraniczne kampanie wpływów oraz kradzież zagranicznych innowacji i technologii wojskowej.

Termin nieograniczona wojna hybrydowa nawiązuje do powstałej w latach 90. ubiegłego wieku strategii, którą stworzyli i opisali dwaj chińscy pułkownicy sił powietrznych Qiao Liang i Wang Xiangsui w książce „Unrestricted Warfare". Wydała ją Armia Ludowo-Wyzwoleńcza, siły zbrojne KPCh. Autorzy korzystali z oryginalnych dokumentów wojskowych. Strategia ta opowiada się za zastosowaniem serii niekonwencjonalnych taktyk, stworzonych po to, by osiągnąć cele wojny jednak bez angażowania się w rzeczywistą walkę.

Jak zauważa Fleming, ostatecznym celem tej strategii jest „zniszczenie demokracji po to, by chiński komunizm mógł globalnie przejąć nadzór".

Dyrektorem naczelnym Zhenhua jest Wang Xuefeng, były inżynier IBM. Jak podaje australijski nadawca ABC, wcześniej w chińskich mediach społecznościowych zamieścił wpis o prowadzeniu „wojny hybrydowej" poprzez manipulowanie opinią publiczną i „wojnę psychologiczną".

Zdaniem Nicholasa Eftimiadesa, byłego wysokiego funkcjonariusza sił wywiadowczych USA i autora książki

„Chinese Intelligence Operations” (pol. „Chińskie operacje wywiadowcze”), baza danych pomogłaby chińskiemu wywiadowi w namierzeniu tych, którzy nadawaliby się do rekrutacji lub szantażu. Chodzi o osoby ze „słabościami”, które można wykorzystać, np. „zapotrzebowanie na pieniądze [lub] sympatie polityczne przeciwne administracji”. Reżim mógłby wyszukiwać w mediach społecznościowych posty, które sugerują niezadowolenie z rządu lub trudności finansowe.

W analogiczny sposób działa to w przypadku operacji wywierania wpływu. Wyszukiwani są ludzie publikujący opinie, które popierają politykę reżimu. Kolejnym krokiem jest wspieranie takiej osoby, jej organizacji, a tym samym wzmacnianie jej poglądów.

Michael Shoebridge zwraca uwagę, że w bazie Zhenhua znajdują się także dane dzieci wpływowych ludzi, m.in. polityków i dyrektorów biznesowych. „To dość niepokojący potencjał wykorzystania takich danych” – zaznacza ekspert. Umożliwia bowiem wywieranie nacisku na te osoby, wykorzystując słabości ich potomstwa.

Ponadto część tych dzieci może w dorosłym życiu piastować eksponowane stanowiska. Zatem na skutek analizowania ich profili już od dzieciństwa „możliwość wykorzystywania tych osób i wpływania na nie jest znacznie większa, ponieważ z biegiem czasu zyskujesz o wiele bardziej wszechstronne ich zrozumienie” – wskazuje Shoebridge.

Kropla w morzu… chińskich baz danych

Eksperci zaznaczają, że gromadzenie danych przez chiński reżim komunistyczny odbywa się na masową skalę, znacznie większą, niż jesteśmy w stanie sobie wyobrazić, a wyciek danych z Zhenhua, to jedynie przysłowiowa kropla w morzu tego, co tam się dzieje.

Shoebridge porównał bazę danych do pojedynczej plastikowej piłeczki w ogromnym basenie. Jak twierdzi, ten zbiór danych

byłby łączony z danymi, które zebrały inne chińskie podmioty w celu ich wykorzystania do różnych operacji, mających wesprzeć interesy reżimu.

„To interakcja firm posiadających takie dane z innymi firmami i danymi rządowymi daje władzę" – skomentował ekspert.

Michael Shoebridge tłumaczy, że strategia ta znajduje odzwierciedlenie w doktrynie reżimu o „fuzji cywilno-wojskowej". Dzięki niej władze wykorzystują innowacje prywatnych przedsiębiorstw do napędzania rozwoju wojskowego.

W październiku 2019 roku Australian Strategic Policy Institute opublikował raport „Engineering global consent", napisany przez Samanthę Hoffman. Stwierdzono w nim, że reżim tworzy „masowy i globalny ekosystem gromadzenia danych", wykorzystując możliwości przedsiębiorstw państwowych i prywatnych chińskich firm technologicznych.

Wymienia się w nim Global Tone Communication Technology Co., spółkę zależną chińskiego przedsiębiorstwa państwowego, nadzorowanego przez centralny wydział propagandy KPCh.

W wywiadzie udzielonym pod koniec zeszłego roku polskiej edycji „The Epoch Times" gen. Robert Spalding powiedział, że Global ToneCommunication, to firma prowadząca usługi tłumaczeniowe, która „w rzeczywistości przy użyciu sztucznej inteligencji gromadzi wielki zbiór danych". Jak dodał: „Czasami ma tę funkcję wbudowaną na podobnych zasadach co produkty Huawei, jako most telekomunikacyjny, lub może bazować na oprogramowaniu opartym na tzw. chmurze".

Poza gromadzeniem ogromnych baz danych z całego świata w ponad 65 językach, które przetwarza na użytek Pekinu do celów wywiadowczych, bezpieczeństwa i propagandy, firma koncentruje się na technologiach sztucznej inteligencji, takich jak rozpoznawanie twarzy.

W opinii Nicholasa Eftimiadesa chińskich firm zaangażowanych

w gromadzenie dużych ilości danych na potrzeby reżimu są prawdopodobnie dziesiątki, jeśli nie setki. Nie wliczając w to działań prowadzonych przez chińskie agencje bezpieczeństwa, które za pośrednictwem zaawansowanego technologicznie aparatu nadzoru tego kraju zbierają dane na temat wszystkich obywateli, a więc 1,4 mld ludzi.

Eftimiades twierdzi, że dane dziesiątek milionów Amerykanów zostały wykradzione przez chińskich hakerów. Zostały one wprowadzone do baz w Chinach i służą do doskonalenia narzędzi sztucznej inteligencji. Wśród ataków wyliczyć można włamanie do amerykańskiego Urzędu Zarządzania Personelem (ang. Office of Personnel Management, OPM) w 2014 roku, federalnej agencji ds. personelu, naruszenie obowiązku sprawozdawczego firmy Equifax w 2017 roku, a także cyberatak na ubezpieczyciela zdrowotnego Anthem w 2016 roku.

W lutym 2016 roku anglojęzyczna edycja „The Epoch Times", powołując się na poufne źródło w Chinach, poinformowała, że chińskie agencje bezpieczeństwa stworzyły bazę danych wykorzystywaną do przetwarzania skradzionych danych Amerykanów. Zawiera ona także poufne dane osobowe, wyszczególnione w poświadczeniach bezpieczeństwa 21 mln obecnych i byłych pracowników federalnych, pochodzące z włamania do Urzędu Zarządzania Personelem (OPM) oraz osobiste dane prawie 80 mln obecnych i byłych klientów i pracowników Anthem.

Ta baza danych funkcjonuje na potężnym oprogramowaniu zdolnym do przyjmowania ogromnych ilości danych. Zgromadzone zasoby analizuje się pod kątem relacji między różnymi osobami i zdarzeniami.

Wyciek danych z Zhenhua Data Technology jest dla wszystkich, niezależnie od statusu społecznego, okazją do zastanowienia się nad zamieszczanymi treściami w mediach społecznościowych. Jak widać, mogą one nieoczekiwanie stać się pożywką dla podmiotów gromadzących dane. Mogą zostać wykorzystane

przeciwko nam, zwłaszcza jeśli trafią do państwa totalitarnego, jakim są Chiny.

Źródła:

Military-Linked Chinese Company Collected Personal Data On Thousands of Canadians

How Chinese Data Trove on 2 Million People Serves Beijing's Unrestricted Warfare

„Gazeta Polska"

The Washington Post

The Globe and Mail

The Guardian