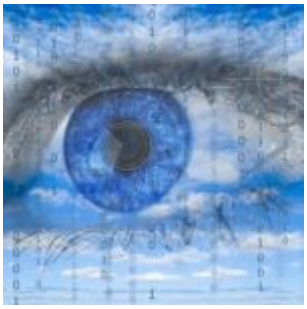
Wielki Brat szpieguje cię na tysiące sposobów, a wszystkie te informacje trafiają do scentralizowanych „systemów fuzyjnych”



Wielki Brat cię obserwuje. Niestety, większość ludzi nie zdaje sobie sprawy, jak rozległa stała się siatka nadzoru. Gdy jedziesz do pracy lub szkoły, czytniki tablic rejestracyjnych systematycznie śledzą Twoją podróż. W dużych miastach tysiące wysoce zaawansowanych kamer bezpieczeństwa (wiele z nich wyposażonych jest w technologię rozpoznawania twarzy) monitoruje każdy Twój ruch. Jeśli władze wykryją, że robisz coś podejrzanego, mogą szybko przejrzeć Twoją dokumentację karną, finansową i medyczną. Oczywiście, jeśli chcą sięgnąć głębiej, telefon i komputer nieustannie tworzą skarbnicę danych z monitoringu. Nic, co robisz na którymkolwiek z nich, nigdy nie jest prywatne.

W przeszłości zebranie wszystkich tych informacji zajmowało dużo czasu. Ale teraz giganci technologiczni, tacy jak Microsoft, Motorola, Cisco i Palantir, sprzedają „systemy fuzyjne” rządom na całym świecie. Te „systemy fuzyjne” mogą natychmiast integrować dane z monitoringu z tysięcy różnych źródeł, a to całkowicie zmieniło sposób, w jaki egzekwowanie prawa jest prowadzone w wielu największych miastach.

Arthur Holland Michel jest starszym wykładowcą w Carnegie Council for Ethics in International Affairs i odbył wycieczkę po „systemie fuzyjnym” używanym przez miasto Chicago o nazwie Citigraf:

> ***Kliknął „ZBADAJ” i Citigraf zabrał się do pracy nad zgłoszonym napadem.*** *Oprogramowanie działa na czymś, co Genetec nazywa „silnikiem korelacyjnym”, czyli zestawem algorytmów, które przeszukują historyczne rejestry policyjne miasta i dane z czujników na żywo w poszukiwaniu wzorców i połączeń. Kilka sekund później na ekranie pojawiła się długa lista potencjalnych klientów, w tym wykaz osób wcześniej aresztowanych w okolicy za brutalne przestępstwa, adresy domowe mieszkających w pobliżu zwolnionych warunkowo, katalog podobnych niedawnych telefonów 911, zdjęcia i numery rejestracyjne pojazdów, które wykryto uciekające z miejsca zbrodni i nagrania wideo z wszelkich kamer, które mogły wykryć dowody samej zbrodni, w tym tych zamontowanych w przejeżdżających autobusach i pociągach. Innymi słowy, więcej niż wystarczająca ilość informacji, aby funkcjonariusz mógł odpowiedzieć na to pierwotne wezwanie pod numer 911 z niemal telepatycznym wyczuciem tego, co właśnie się wydarzyło.*

Ale te systemy służą nie tylko do tropienia przestępców.

W rzeczywistości można ich użyć do zbadania dosłownie każdego.

Przy innej okazji Arthur Holland Michel miał okazję przetestować „system fuzyjny”, który Microsoft zbudował dla Nowego Jorku:

> *Funkcjonariusz NYPD pokazał mi, w jaki sposób może wyciągnąć kartotekę każdego mieszkańca miasta, listy jego znanych współpracowników, przypadki, w których zostali nazwani ofiarą przestępstwa lub świadkami, a jeśli mieli samochód, mapę cieplną gdzie zwykle prowadzili i pełną historię ich naruszeń parkingowych. Potem wręczył mi telefon. Śmiało, powiedział; wyszukaj nazwisko.*

> *Przyszła mi do głowy fala ludzi: przyjaciele. Kochankowie. Wrogowie. W końcu wybrałem ofiarę strzelaniny, której byłem świadkiem na Brooklynie kilka lat wcześniej. Pojawił się od razu, wraz z tym, co wydawało się bardziej osobistymi informacjami niż ja, a może nawet ciekawy funkcjonariusz, miałam prawo wiedzieć bez nakazu sądowego. Czując zawroty głowy, oddałem telefon.*

Jeśli tak się dzieje w dużych miastach, takich jak Chicago i Nowy Jork, czy możesz sobie wyobrazić technologię, którą muszą teraz posiadać agencje alfabetu rządu federalnego?

Oczywiście dzieje się to nie tylko w Stanach Zjednoczonych.

Po drugiej stronie Atlantyku wspólny europejski projekt nadzoru znany jako ROXANNE budzi wiele obaw:

> *Akronim **R**eal time netw**O**rk, te**X**t, and speaker **AN**alytics for combating orga**N**ized crim**E** (Analiza sieci, tekstu i mowy w czasie rzeczywistym w celu zwalczania przestępczości zorganizowanej), został ogłoszony w listopadzie w ramach projektu opracowanego obecnie w Szwajcarii.*
>
> *Platforma biometryczna rzekomo służąca do monitorowania i rozprawiania się z przestępczością zorganizowaną, dodatkowe zastosowanie ROXANNE, które jego twórcy swobodnie reklamują, jest możliwość monitorowania osób winnych rzekomej mowy nienawiści i politycznego ekstremizmu.*

W całej Europie wprowadzane są nowe, surowe przepisy przeciwko „mowie nienawiści" i „ekstremizmowi politycznemu", a to nowe narzędzie pomoże wytropić „myślozbrodniarzy".

W szczególności to nowe narzędzie będzie intensywnie monitorować „serwisy społecznościowe, takie jak Facebook, YouTube, a także zwykłe platformy telekomunikacyjne"…

> *ROXANNE, produkt finansowany przez UE w ramach programu*

> *„Horyzont 2020", mający na celu wspieranie nowej technologii nadzoru, działa na portalach społecznościowych, takich jak Facebook, YouTube, a także na zwykłych platformach telekomunikacyjnych, aby identyfikować, kategoryzować i śledzić twarze i głosy, umożliwiając władzom stworzenie bardziej szczegółowego obrazu badanej sieci, czy to w związku z działalnością przestępczą, czy też uznaną za politycznie skrajną.*

> *Umożliwienie władzom czerpania z surowych danych z różnych źródeł i platform w celu rozpoznania typowych wzorców mowy, rysów twarzy i geolokalizacji, rezultatem końcowym jest zarówno identyfikacja podejrzanych, jak i nakreślenie skomplikowanego obrazu sieci poddawanych pod mikroskop.*

Jeśli więc mieszkasz w Europie i uważasz, że w pewnym momencie możesz być winny „myślozbrodni", możesz chcieć pozbyć się telefonu i komputera.

Poważnie.

Tam naprawdę źle się potoczyło i to tylko kwestia czasu, zanim szaleństwo w Stanach Zjednoczonych osiągnie ten sam poziom, ponieważ idziemy dokładnie tą samą drogą.

W Stanach Zjednoczonych, z każdym dniem coraz więcej głosów politycznych jest „obniżanych". Postępowy reporter Jordan Chariton początkowo wiwatował, gdy konserwatyści byli odrzucani, ale w tym momencie żałuje, że wezwał do cenzury teraz, gdy YouTube usunął jeden z jego filmów:

> *Jednak po tym, jak YouTube usunął wideo z jego własnego kanału, przedstawiające materiał z zamieszek 6 stycznia za naruszenie zasad platformy przeciwko „spamowi i nieuczciwym praktykom", Chariton zmienił swoje stanowisko.*

> *„Mając czas na refleksję i widząc atak cenzury Doliny Krzemowej, żałuję tego tweeta" – napisał progresywny*

dziennikarz. „Niezależnie od tego, czy niektóre kanały telewizji kablowej/YouTube wprowadzają w błąd widzów, przedstawiając nieuczciwe twierdzenia pozbawione prawdziwych dowodów, nie należy ich atakować”

To wszystko jest zabawne, kiedy dzieje się „po drugiej stronie”, ale kiedy ci się to przytrafia, nagle staje się rzeczywistością.

Naprawdę chcą kontrolować to, co wszyscy robimy, mówimy i myślimy, a siatka nadzoru Wielkiego Brata staje się coraz bardziej dusząca z każdym mijającym rokiem.

Jeśli nie ograniczymy tej technologii, póki jeszcze możemy, to tylko kwestia czasu, zanim nasze społeczeństwo stanie się dystopijnym koszmarem o wiele straszniejszym niż cokolwiek, co George Orwell kiedykolwiek odważył się wyobrazić.

Artykuł przetłumaczono z zerohedge.com

Czy szczepionka na COVID-19 będzie bezpieczna?

Coraz więcej osób pyta mnie, czy proponowana szczepionka na SarsCoV-2 będzie bezpieczna. Jest nowatorska (po raz pierwszy w historii ma to być szczepionka wpływająca na geny). Nie było

możliwości wieloletniej obserwacji i dłuższych badań, jak to jest wymagane przy wprowadzaniu na rynek nowej szczepionki. Nie mogę więc mieć informacji na temat jej bezpieczeństwa i ewentualnych odległych skutków ubocznych – z prostego powodu – nie ma ich nikt na świecie. Mogę się opierać na materiałach udokumentowanych, dotyczących tego tematu i takie też informacje mogę obiektywnie przekazywać. Nasze władze informują, że szczepionka będzie bezpieczna. Posłowie kilku klubów zadali w Sejmie dużo konkretnych pytań dotyczących szczepienia na Covid19.

(https://www.sejm.gov.pl/sejm9.nsf/InterpelacjaTresc.xsp…)

Zacytuję pytanie nr 21: „Pan Premier powiedział publicznie, że według danych naukowców z firmy Pfizer – szczepionka nie ma skutków ubocznych. Pan Premier zaufał im na słowo, czy jest w posiadaniu jakichkolwiek badań, dowodów na potwierdzenie tej tezy?”Firma Pfizer rzeczywiście zapewnia, że szczepionka może być szeroko stosowana na całym świecie (https://www.money.pl/…/szczepionka-na-koronawirusa…).

Tymczasem federalni prokuratorzy USA określili tę firmę mianem notorycznego oszusta i przestępcy. Firma została wielokrotnie ukarana (wypłaciła miliardy dolarów kar) za wprowadzanie w błąd w kwestii zastosowania wielu leków (np. Zoloft, Lipitor, Lyrica, Bextra). Zarzut dotyczył także nielegalnego testowania antybiotyków na dzieciach w Nigerii. Firma była zainteresowana zwiększeniem wyników sprzedaży nie licząc się ze zdrowiem i bezpieczeństwem pacjentów.W zdecydowanej większości krajów Europy są instytucje, które finansują leczenie osób dotkniętych powikłaniami poszczepiennymi. W Polsce takiej instytucji nie ma. Jej powstanie jest skutecznie blokowane (https://wpolityce.pl/…/528159-notoryczny-oszust-i…).

Firma AstraZeneca przyznaje wprost, że skutki uboczne po szczepionce na SarsCoV-2 mogłyby ujawnić się nawet po kilku latach i dlatego firma nie może wziąć na siebie ŻADNEJ odpowiedzialności za ewentualne powikłania

(https://www.politykazdrowotna.com/62459,astrazeneca…).

Podsumowując: w razie powikłań pacjent zostanie sam ze swoimi chorobami licząc na opiekę totalnie niewydolnych placówek ochrony zdrowia. A gdyby nawet zmarł w wyniku powikłań, to nikt nie zapłaci odszkodowania.Polscy naukowcy i lekarze, podchodząc bardzo merytorycznie do problemu w liście otwartym do Prezydenta i Rządu twierdzą, że szczepienia na koronawirusa NIE SĄ BEZPIECZNE.

„Szczepionki nie zostały właściwie zbadane i ich zastosowanie może doprowadzić do nieoczekiwanych zmian zarówno na poziomie komórkowym, w tym zmian szlaków sygnałowych i zmiany ekspresji genów" – czytamy w piśmie."Wprowadzane obecnie pośpiesznie szczepionki mają charakter eksperymentu na wielką skalę. Ponieważ mogą obniżyć naszą odporność na inne choroby, na skutek masowych szczepień może więc umrzeć więcej ludzi niż obecnie na COVID-19. Ponadto zmiany genetyczne wywołane przez szczepionki mogą wpłynąć na przyszłe pokolenia" (https://dorzeczy.pl/…/lekarze-i-naukowcy-ostrzegaja…).

Autor: *Marcin Lis*

UOKiK radzi na co uważać, kupując przez internet świąteczne prezenty

Zamawiając prezenty świąteczne przez internet np. spoza UE przez platformy sprzedażowe, warto sprawdzić, kto jest sprzedawcą i za co odpowiada polski sklep. Jeśli sprzedawca jest w Azji, mogą być problemy z dochodzeniem praw – ostrzega UOKiK.

W czwartkowym komunikacie Urząd Ochrony Konkurencji i Konsumentów (UOKiK) radzi, by przed skorzystaniem z oferty sklepu internetowego typu: „Prosto od zagranicznego producenta, tanio", „Nasi sprzedawcy z Azji", „Klient jest importerem towaru", sprawdzić dane przedsiębiorcy, gdzie ma siedzibę, czas dostawy. Warto upewnić się, że nie mamy do czynienia jedynie z pośrednikiem, który za nic nie odpowiada.

„W tym roku wiele osób, aby zminimalizować ryzyko zakażenia koronawirusem (wirusem KPCh – przyp. redakcji), będzie zamawiać prezenty świąteczne przez internet. Niektóre z nich mogą być sprowadzane spoza Unii Europejskiej przez platformy sprzedażowe działające w modelu dropshippingu. Polega on na tym, że konsument ma do czynienia z dwoma przedsiębiorcami" – powiedział prezes UOKiK Tomasz Chróstny, cytowany w komunikacie. Wyjaśnił, że pierwszy to przeważnie sklep internetowy zarejestrowany w Polsce. Drugi to najczęściej przedsiębiorca z siedzibą na Dalekim Wschodzie, np. w Chinach.

„Bardzo ważne jest, aby przed zakupem sprawdzić w regulaminie, kto tak naprawdę jest sprzedawcą i za co odpowiada polski sklep. Jeśli sprzedawca jest w Azji, bądźmy świadomi, że mogą powstać problemy z dochodzeniem naszych praw konsumenckich" – podkreślił.

Szef UOKiK zaapelował do konsumentów, by zwracali uwagę, z kim zawierają umowę i kto odpowiada za jej realizację. „Jeśli na stronie internetowej lub w regulaminie pojawiają się zapisy typu ‘sprzedawca towaru z Azji’ czy ‘klient jako importer towaru uiszcza opłaty celno-skarbowe’, konsumentowi powinna się zapalić czerwona lampka” – zwraca uwagę UOKiK.

Jeśli klient zdecyduje się na zakup, musi mieć świadomość, że w przypadku problemów, np. z wysyłką czy wadliwym towarem, reklamację będzie składał w Azji i może mieć problem z jej wyegzekwowaniem – przypomina Urząd.

Warianty dropshippingu

Eksperci UOKiK zweryfikowali regulaminy sklepów działających w modelu dropshippingu. Wskazali na kilka wariantów dropshippingu. W pierwszym przedsiębiorca A jest sprzedawcą, a przedsiębiorca B – dostawcą i taka sytuacja jest najkorzystniejsza dla konsumentów, bo za wszystko odpowiada polska firma i obowiązuje polskie prawo konsumenckie. Przed transakcją można sprawdzić przedsiębiorcę, a w razie ewentualnych problemów – dochodzić roszczeń od sklepu, który jest na miejscu.

W sytuacji kiedy przedsiębiorca A jest pośrednikiem, ale działa w imieniu i na rzecz konsumenta, a przedsiębiorca B jest sprzedawcą, polski sklep wyraźnie wskazuje w regulaminie, że bierze na siebie niektóre lub wszystkie obowiązki sprzedawcy. „Optymalne dla konsumenta jest, aby to polski przedsiębiorca odpowiadał np. za wady towaru z tytułu rękojmi, za dostarczenie zakupów w określonym czasie czy przyjmował zwroty w przypadku odstąpienia od umowy” – wskazał UOKiK.

Trzeci wariant, w którym przedsiębiorca A jest tylko pośrednikiem, a przedsiębiorca B – sprzedawcą, to najczęstsza i najmniej korzystna sytuacja dla konsumentów. Pośrednik ma wobec nich tylko takie obowiązki, jakie wpisał do regulaminu. Czasami nie wpisuje żadnych. W tym wariancie

konsumenci często muszą samodzielnie wysyłać zwroty produktów lub reklamacje do dalekich krajów, gdzie mogą obowiązywać odmienne przepisy.

Chróstny zaapelował do polskich przedsiębiorców, aby konstruując regulaminy swoich e-sklepów, korzystali z wzorców, które są przyjazne, korzystne i przejrzyste dla konsumentów, aby brali na siebie obowiązki sprzedawców dotyczące reklamacji czy odstąpienia od umowy. „Taka postawa im się opłaci. Przy dużej konkurencji na rynku e-commerce konsumenci docenią, że nie są odsyłani z problemami do Chin i chętniej będą korzystać z oferty rzetelnych sklepów" – podkreślił prezes UOKiK.

Urząd radzi, by przed zakupem sprawdzić m.in., czy na stronie sklepu jest regulamin; jeśli nie ma, to najlepiej tam nie kupować, bo nie wiadomo, jakie są prawa i obowiązki; jeśli jest, powinno się go dokładnie przeczytać i zwrócić uwagę, kto jest stroną umowy (sprzedawcą). Warto też sprawdzić, czy na stronie są kompletne informacje o sprzedawcy. Brak pełnej nazwy, siedziby czy danych kontaktowych może oznaczać, że sklep chce coś ukryć, np. że ma siedzibę poza UE. Podawanie danych i adresu przedsiębiorcy lub przedsiębiorcy, na którego rzecz działa, jest ustawowym obowiązkiem.

Dobrze jest zweryfikować również, czy firma ma siedzibę w Europejskim Obszarze Gospodarczym – w takim przypadku obowiązują prawa konsumenckie bardzo podobne do tych w Polsce, a w dochodzeniu roszczeń pomoże działające przy UOKiK Europejskie Centrum Konsumenckie.

W przypadku gdy klient miał do czynienia z nieuczciwym przedsiębiorcą internetowym, a płacił kartą, może odzyskać pieniądze dzięki tzw. procedurze chargeback, składając reklamację do banku. Jeśli zobaczy jakąś podejrzaną stronę, może zawiadomić firmę hostingową lub rejestratora domeny. Ich dane można ustalić na stronie: www.dns.pl lub whois.domaintools.com (dla domen zagranicznych). Jeśli dojdzie

do oszustwa, powinno się zawiadomić organy ścigania – policję, prokuraturę.

UOKiK przypomina, że konsumenci mogą uzyskać pomoc pod numerami tel.: 801 440 220 lub 22 290 89 16 (infolinia konsumencka), pod adresem e-mail: porady@dlakonsumentow.pl, u rzeczników konsumentów, w Europejskim Centrum Konsumenckim, tel.: 22 55 60 600 – w sprawach transgranicznych dotyczących państw UE, Norwegii, Islandii i Wielkiej Brytanii.

Źródła: PAP, UOKiK.

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

Ekspert UODO: Podczas lekcji online dbajmy o swą prywatność

Podczas lekcji online uczniowie i nauczyciele powinni dbać o swoją prywatność. Kamerka internetowa powinna pokazywać jak najmniej z ich otoczenia – zaleca radca Urzędu Ochrony Danych Osobowych Piotr Drobek. Przypomina, że uczniowie i rodzice nie mogą bez zgody nauczyciela publikować w sieci nagrań zdalnych lekcji.

Od poniedziałku zdalne nauczanie wróciło na większą skalę: w szkołach średnich w czerwonej strefie jest obowiązkowe, w liceach i technikach w żółtej strefie ma być łączone z nauką w szkolnych murach. W czwartek ma być ogłoszona decyzja w sprawie szkół podstawowych. Zgodnie z zapowiedziami premiera Mateusza Morawieckiego, wyższe klasy podstawówek będą uczyć się zdalnie lub w systemie hybrydowym.

Drobek zaznaczył w rozmowie z PAP, że zdalne kształcenie i wykorzystywane do tego narzędzia rodzą nowe zagrożenia związane z ochroną danych osobowych w oświacie. Uwydatniły się też problemy, które w wielu szkołach nie były wcześniej rozwiązane, jak to, czy nauczyciel może korzystać z prywatnego sprzętu w domu, np. logując się do elektronicznego dziennika.

„Warto podkreślić, że RODO nie zakazuje wykorzystywania sprzętu prywatnego. Szkoła powinna wprowadzić zasady posługiwania się takim sprzętem i przeprowadzić szkolenia nauczycieli, jak mają bezpiecznie z niego korzystać” – powiedział Drobek.

Dodał, że wykorzystywanie dziennika elektronicznego do kontaktowania się z rodzicami zapewnia większe bezpieczeństwo niż używanie poczty elektronicznej i wyklucza wcześniej zdarzające się często naruszenia, jak wysyłanie korespondencji zbiorowej z podaniem wszystkich adresatów.

Ekspert podkreślił, że bez względu na to, czy nauka odbywa się w szkolnym budynku, czy jest prowadzona zdalnie, administratorem danych osobowych jest szkoła, a kierujący placówką dyrektor odpowiada za bezpieczeństwo ich przetwarzania.

„Nauczyciel nie jest odrębnym administratorem danych, dlatego jeśli wykorzystuje narzędzia zdalnej edukacji, powinien

to robić w porozumieniu z dyrektorem szkoły” – wskazał.

„Większość szkół, przechodząc na zdalną edukację, nie miało wdrożonych ani nie wdrożyło w jednolity sposób służących do tego celu platform lub narzędzi. Z tego powodu poszczególni nauczyciele samodzielnie wybierali narzędzia lub aplikacje wykorzystywane do zdalnej edukacji, choć nie zawsze byli w stanie zdiagnozować ryzyko związane z ich wykorzystywaniem” – mówił Drobek.

Zaznaczył, że z czasem coraz więcej szkół, a także organów prowadzących, zaczęło wprowadzać w swoich placówkach jednolite platformy edukacyjne czy aplikacje.

„To pozwala zapewnić bezpieczeństwo w ramach jednego narzędzia, bez względu na to, jakie nauczyciele czy uczniowie mają umiejętności” – wskazał radca UODO.

Oprócz określenia jednolitego narzędzia do edukacji zdalnej szkoły powinny też ustalić zasady ochrony danych osobowych podczas zdalnych lekcji, wskazać, jak nauczyciel powinien reagować w sytuacji np. nagrywania lekcji czy naruszenia ochrony danych osobowych.

Ekspert zwrócił uwagę, że rodzic może w porozumieniu z nauczycielem nagrać lekcję online po to, by np. utrwalić z dzieckiem wiedzę czy odrobić lekcje. W żadnym wypadku takie nagranie nie może być jednak bez zgody nauczyciela udostępnione w sieci – ani przez rodzica, ani przez ucznia.

Drobek zauważył, że uczniom powinno się też przypominać o zachowaniu prywatności podczas korzystania z mediów społecznościowych czy gier sieciowych, a także podczas lekcji online.

„Pamiętajmy, kiedy podczas lekcji online korzystamy z kamerek internetowych, w taki sposób zaaranżujmy swoje otoczenie, żeby zachować swoją prywatność. Zastanówmy się, jakie elementy niekoniecznie chcemy pokazywać klasie” – zalecił uczniom.

Dodał, że o tym samym powinni pamiętać nauczyciele.

Autor: *Karolina Mózgowiec*

Szwecja zakazała wykorzystywania sprzętu Huawei i ZTE do budowy sieci 5G

W Szwecji urząd nadzoru telekomunikacyjnego ogłosił we wtorek, że w budowaniu sieci 5G w tym kraju zakazane będzie korzystanie ze sprzętu chińskich koncernów telekomunikacyjnych Huawei i ZTE lub ich dostawców. To kolejne państwo europejskie, które zdecydowało się na taki krok.

Urząd poczty i telekomunikacji poinformował o tej decyzji przy okazji ogłoszonych w Szwecji na 10 listopada aukcji częstotliwości umożliwiających rozwój sieci 5G.

Regulator zakazał stosowania produktów dwóch chińskich firm do nowych instalacji telekomunikacyjnych tworzonych na potrzeby obsługiwania tych kontraktów. Do 2025 roku również będzie musiał zostać wycofany sprzęt produkcji Huawei i ZTE, który już jest w Szwecji używany i wykorzystywany w tym celu.

Decyzję podjęto na podstawie obowiązującej od początku roku nowej ustawy, po przeprowadzeniu konsultacji z wojskiem i służbami specjalnymi, „by zapewnić, że używanie sprzętu radiowego w tych pasmach nie przyczyni się do narażenia bezpieczeństwa Szwecji”.

USA starają się przekonać swoich sojuszników do wykluczania chińskich firm z budowy infrastruktury telekomunikacyjnej, uzasadniając to obawami o bezpieczeństwo danych. Koncerny z ChRL muszą zgodnie z tamtejszym prawem pomagać państwu w zbieraniu danych wywiadowczych – przypomina Reuters.

Na całkowitą rezygnację z używania produktów Huawei do 2027 roku zdecydowała się w tym roku Wielka Brytania, kilka innych krajów europejskich podjęło lub zamierza podjąć podobne działania – pisze AFP.

Na decyzji szwedzkiego regulatora najprawdopodobniej skorzystają szwedzki koncern Ericsson i fińska Nokia również produkujące sprzęt wykorzystywany do budowy infrastruktury 5G.

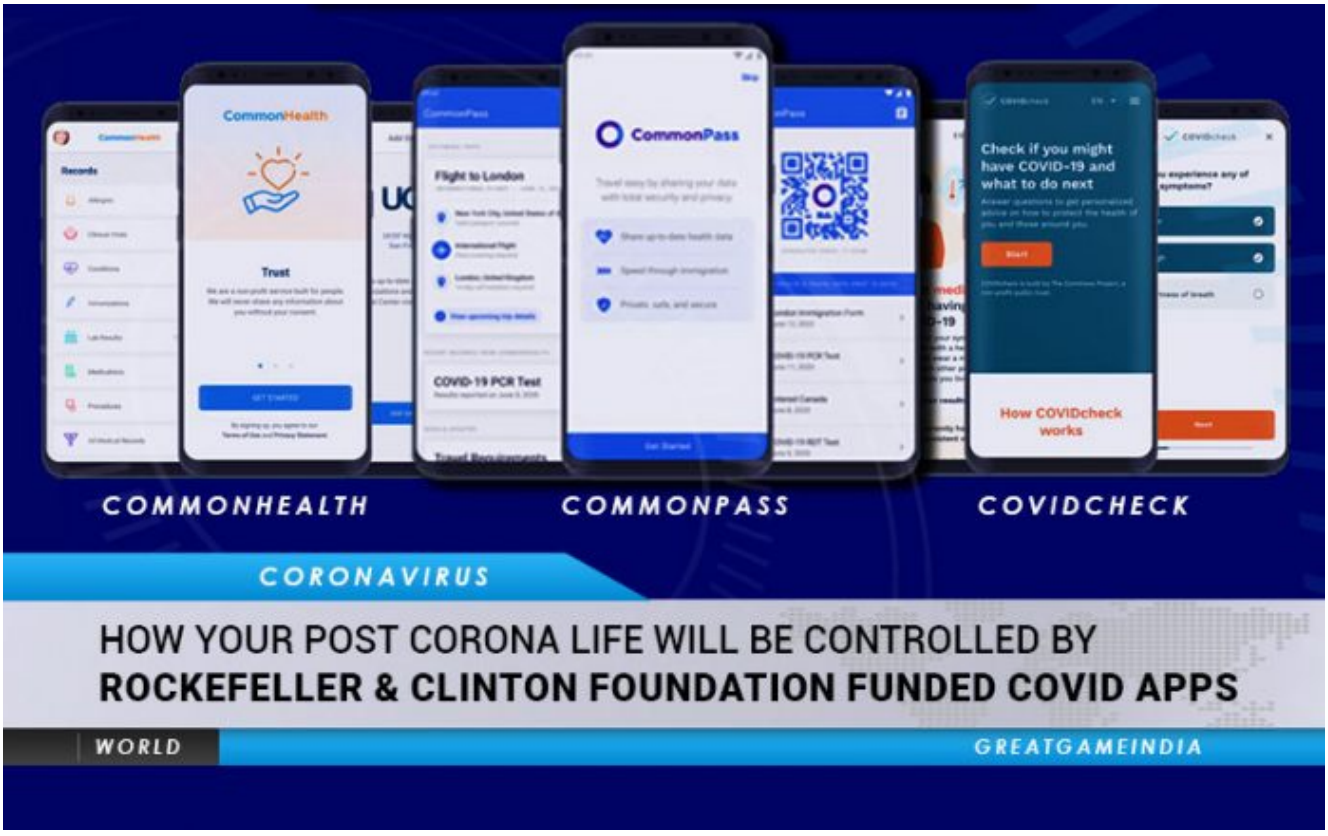
Źródło:

PAP

Jak Twoje poCOVIDowe życie będzie kontrolowane przez aplikacje finansowane przez Rockefellera & Clinton

Foundation

Rockefeller Foundation oraz the Clinton Foundation opracowały serię COVID aplikacji, które będą ściśle kontrolować twoje post-covid'owe życie. Inicjatywa została uruchomiona przez fundację non-profit Commons Project Foundation, która jest częścią Światowego Forum Ekonomicznego. Projekt Commons obejmuje trzy aplikacje COVID – CommonHealth, COVIDcheck i CommonPass. Razem będą gromadzić, przechowywać i monitorować dane dotyczące zdrowia, na podstawie których aplikacje zdecydują, czy możesz podróżować, uczyć się, chodzić do biura itp.



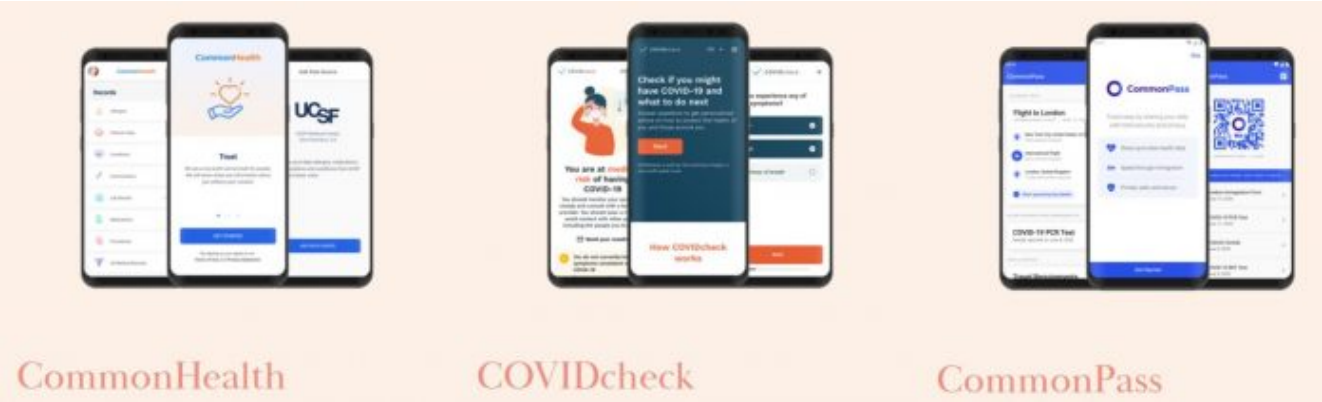
Projekt Commons

Projekt Commons jest publicznym funduszem non-profit założonym przy wsparciu Fundacji Rockefellera w celu budowania platform i usług, które będą ściśle regulować twoje post-covid'owe życie. Inicjatywa jest częścią Światowego Forum Ekonomicznego realizującego program The Great Reset.

Na stronie www The Commons Project tak opisują swoją rolę:

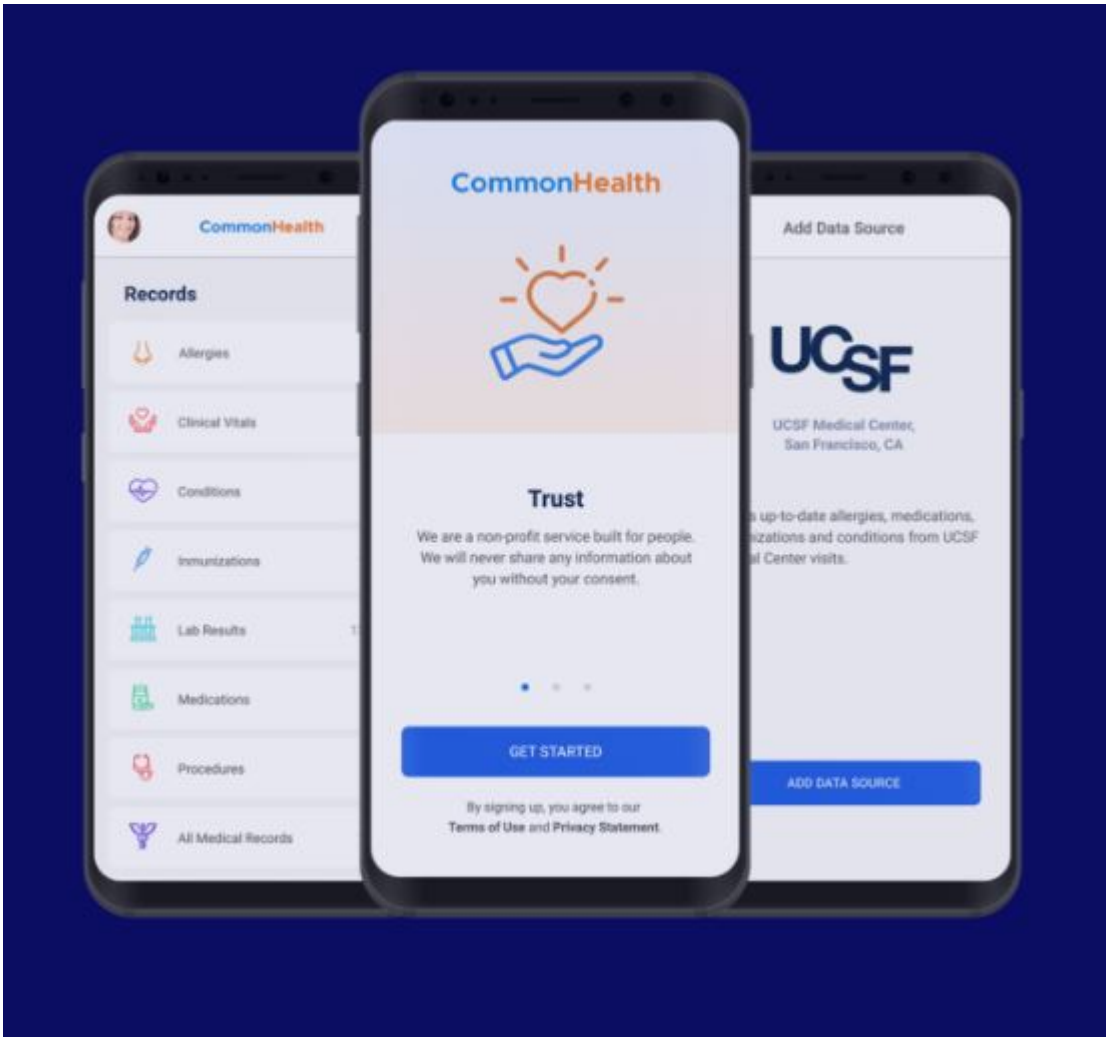
Projekt Commons jest publicznym funduszem non-profit, ustanowionym przy wsparciu ***Fundacji Rockefellera w*** *celu tworzenia usług cyfrowych, które stawiają ludzi na pierwszym miejscu.*

Projekt Commons wypełnia lukę między firmami technologicznymi, agencjami rządowymi i tradycyjnymi organizacjami non-profit w celu tworzenia i obsługi usług cyfrowych, które stanowią infrastrukturę publiczną w erze cyfrowej.



CommonHealth

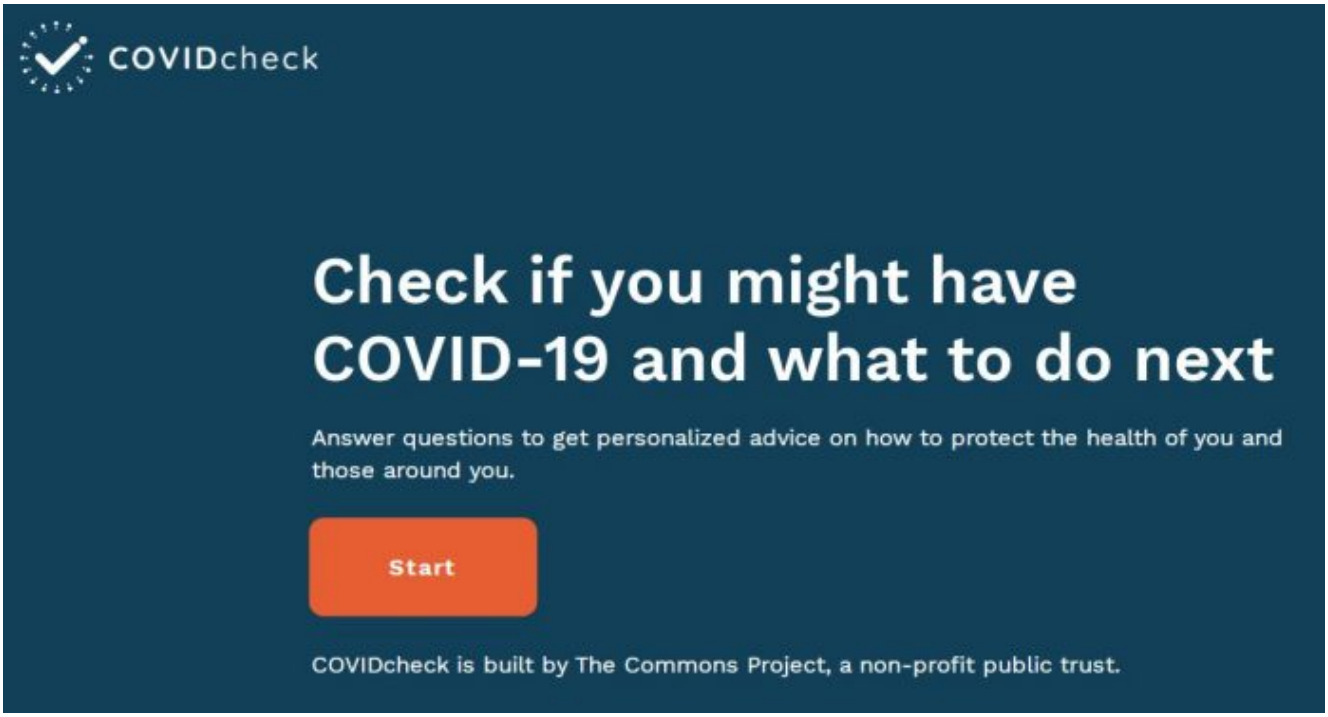
CommonHealth będzie gromadzić i zarządzać Twoimi osobistymi danymi zdrowotnymi oraz udostępniać je służbie zdrowia, organizacjom i innym aplikacjom. Celem CommonHealth jest rozszerzenie modelu przenoszenia danych zdrowotnych i współdziałania, którego pionierem jest Apple Health, na 73% ludzi na całym świecie korzystających z urządzeń z Androidem.



Został opracowany we współpracy z UCSF, Cornell Tech i Sage Bionetworks.

COVIDcheck

COVIDcheck został opracowany we współpracy z CDC, Clinton Foundation i World Medical Association. Stworzy nową normę dla szkół, uniwersytetów, pracodawców i agencji zdrowia publicznego poprzez zestaw pytań, które zadecydują, co należy zrobić dalej.



CommonPass

CommonPass to cyfrowy paszport zdrowotny, który będzie posiadał certyfikat testu na COVID-19 lub pokaże, czy zostałeś zaszczepiony, a w przyszłości czy „jesteś zgodny" z różnymi przepisami różnych rządów.

Przepustka działa, gdy pasażerowie przechodzą test w certyfikowanym laboratorium przed przesłaniem. Generuje kod QR, który może zostać zeskanowany przez personel linii lotniczej i funkcjonariuszy granicznych. Będzie to jednak wymagało od rządów zaufania do testów koronawirusa przeprowadzonych w zagranicznych laboratoriach. Na podstawie Twojego statusu CommonPass możesz mieć pozwolenie na podróż lub nie.

https://www.youtube.com/embed/hvHxMA1kA-g
Tymczasem technologia paszportowa CommonPass COVID jest już testowana podczas lotów z lotniska Heathrow.

Operacja Rockefellera Lockstep

W 2010 roku Fundacja Rockefellera sfinansowała ćwiczenie

planowania scenariuszy, które pokazuje, jak globalne elity mogą manipulować polityką publiczną i wpływać na nią podczas pandemii.

Teks w j. angielskimPobierz

Dokument „Scenariusze przyszłości technologii” przewiduje cztery narracje scenariuszowe, z których jedna, nazwana „Krok po kroku”, dotyczy globalnej pandemii. Ten dokument jest uważany przez wielu za rodzaj „instrukcji operacyjnej”, podręcznika opisującego, jak stworzyć nową normalność po wybuchu globalnej pandemii.

Wszystko zdaje się łączyć w całość i prawdziwe oblicze medialnego wirusa zaczyna nabierać rumieńców. Jedno jest pewne, powoli zbliżamy się do kolejnego etapu globalnego zniewolenia.

Źródło:

greatgameindia.com

Kobieta z Teksasu doznała poważnych oparzeń po zapaleniu się środka odkażającego do rąk

Ludzie używają różnych środków czyszczących i środków ochrony zdrowia, aby zapobiec rozprzestrzenianiu się koronawirusa z Wuhan (COVID-19). Eksperci zalecają dokładne mycie rąk, ale jeśli nie masz dostępu do mydła i bieżącej wody to środek

dezynfekujący do rąk jest odpowiednią alternatywą.

Wygląda jednak na to, że konsumenci muszą uważać, jakiej marki środki odkażające do rąk kupują, zwłaszcza po tym, jak kobieta w Teksasie trafiła do szpitala po zapaleniu się środka do dezynfekcji rąk, którego używała.

Butelka odkażacza do rąk eksplodowała

Według lokalnego stowarzyszenia *CBS, KHOU-TV*, Kate Wise doznała poważnych poparzeń całego ciała po incydencie z użyciem środka do dezynfekcji rąk.

Według Wise, mieszkanki Round Rock w Teksasie, do incydentu doszło 30 sierpnia, w niedzielę, po zastosowaniu niemarkowego środka do dezynfekcji rąk, który kupiła, aby chronić siebie i swoje trzy córki przed koronawirusem.

Jednak po użyciu środka dezynfekującego do rąk jej ręka zapaliła się, gdy zapaliła świecę. Według Wise'a płomienie świecy zetknęły się z butelką środka odkażającego, która następnie eksplodowała.

W ciągu kilku sekund po wybuchu ogień rozprzestrzenił się nie tylko na jej twarz, ale także na resztę ciała. Mówi, że w tym momencie jej dwie najmłodsze córki pobiegły do □□sąsiadów po pomoc.

W końcu Wise była w stanie zdjąć płonące ubrania i wyprowadzić z domu niepełnosprawną córkę i zwierzęta. Przypominając sobie, co się stało, Wise ostrzegła, że zrobienie czegoś tak prostego, jak zapalenie świecy, może być ryzykowne, gdy w grę wchodzi łatwopalny środek dezynfekujący do rąk.

The Round Rock Fire Department bada przyczyny pożaru.

Trudna i kosztowna droga do wyzdrowienia

Aby pomóc w pokryciu kosztów leczenia, przyjaciółka Wise, Kathryn Bonesteel, założyła stronę GoFundMe.

13 września, w niedzielę, Wise opublikował na swojej stronie podziękowanie hojnym darczyńcom. Obecnie jest w domu w trakcie rekonwalescencji przed kolejną operacją, która obejmuje przeszczep skóry.

Bonesteel od tego czasu ostrzegał innych przed kupowaniem produktów niemarkowych.

„Wszyscy kupujemy to, co jest łatwo dostępne" – powiedziała. „Szukamy sklepów, którym ufamy, takich jak Amazon, aby kupować produkty, których potrzebujemy, aby chronić siebie i nasze rodziny".

Wise ma nadzieję, że podnosząc świadomość, może pomóc innym konsumentom zachować bezpieczeństwo podczas plandemii. „To coś, czego nigdy nie chcesz, aby Twoje dzieci zobaczyły" – ubolewa Wise.

FDA ostrzega przed niebezpiecznymi środkami do dezynfekcji rąk

Eksperci ostrzegają, że łatwopalne płyny i bezpośrednie światło słoneczne mogą spowodować wybuch środka dezynfekującego do rąk. Sherrie Wilson, emerytowany strażak z Dallas, ostrzega, że □□produkt jest zarówno łatwopalny, jak i drażniący.

FDA opublikowała listę marek środków do dezynfekcji rąk, których Amerykanie powinni unikać, ponieważ mogą zawierać substancje toksyczne.

Oprócz toksyn niektóre środki odkażające do rąk na liście zawierają również metanol, związek alkoholowy używany do produkcji paliwa. Oprócz tego, że jest wysoce łatwopalny, metanol jest również niebezpieczny, gdy jest wchłaniany przez skórę, wdychany lub spożywany.

Ponadto FDA ostrzega również, że niektóre marki mogą nie być wystarczająco silne, aby zabić koronawirusa. Lista środków

odkażających, których ludzie powinni unikać, została ostatnio rozszerzona do co najmniej 100 marek i prawie 150 odmian.

Środki ostrożności przy wyborze środka dezynfekującego do rąk

Jak dowodzi incydent z Wise, nie wszystkie środki odkażające do rąk są bezpieczne do regularnego stosowania.

Poniżej znajduje się kilka rzeczy, które należy wziąć pod uwagę przed zakupem środka odkażającego do rąk:

- Według CDC środki do dezynfekcji rąk powinny zawierać co najmniej 60 procent alkoholu etylowego lub 70 procent alkoholu izopropylowego.
- FDA dodaje, że inne zatwierdzone składniki mogą obejmować sterylną wodę destylowaną, nadtlenek wodoru i glicerynę.
- Oprócz metanolu należy również unikać środków do dezynfekcji rąk zawierających **1-propanol** , który może być silnie toksyczny.
- FDA ostrzega również przed stosowaniem środków dezynfekujących do rąk pakowanych w pojemniki na żywność i napoje. Przypadkowe połknięcie tych produktów może być niebezpieczne.
- Według przedstawicieli służby zdrowia należy unikać środków do dezynfekcji rąk, które zastępują alkohol chlorkiem benzalkoniowym, który jest mniej skuteczny w zabijaniu niektórych bakterii i wirusów.
- Tworząc własne środki odkażające, postępuj zgodnie z instrukcjami i używaj odpowiednich składników. Niewłaściwa mieszanka chemikaliów może wytworzyć nieskuteczną mieszaninę lub spowodować oparzenia skóry.

Barun Mathema, badacz chorób zakaźnych z *Columbia University*, namawiał ludzi do używania środka odkażającego do rąk tylko wtedy, gdy nie mogą myć rąk mydłem i wodą, ponieważ dokładne

mycie rąk jest nadal najskuteczniejszym sposobem pozbycia się zarazków.

Źródła:

CBSNews.com 1

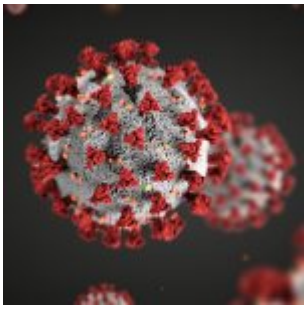
GoFundMe.com

KHOU.com

CBSNews.com 2

FoxNews.com

Niedobór witaminy D jest powiązany z wyższym ryzykiem COVID-19 i poważnymi powikłaniami



Powszechnie wiadomo, że witamina D pełni kilka ważnych funkcji, od wzmacniania odporności organizmu po regulację ciśnienia krwi. W ciągu ostatniej dekady liczne badania dostarczyły również dowodów na to, że przyjmowanie witaminy D może zmniejszyć ryzyko rozwoju infekcji, takich jak przeziębienie i grypa.

Biorąc pod uwagę te precedensy i trwającą pandemię, naukowcy chcą ustalić, czy również witamina D może pomóc w ochronie przed COVID-19, chorobą wywoływaną przez koronawirusa z Wuhan. W niedawnym badaniu naukowcy z Irlandii i Wielkiej Brytanii przyjrzeli się występowaniu niedoborów witaminy D w krajach europejskich o różnym nasileniu zakażenia COVID-19 i odkryli istotną korelację między poziomami witaminy D a ryzykiem i śmiertelnością COVID-19 .

Optymalizacja poziomu witaminy D może przynieść potencjalne korzyści pacjentom z COVID-19

Naukowcy zauważyli związek po przeanalizowaniu badań dotyczącym poziomu witaminy D u osób starszych w krajach europejskich dotkniętych COVID-19. Naukowcy wybrali kraje na podstawie ich wskaźników infekcji. Zespół uzyskał również wskaźniki śmiertelności COVID-19 w tych krajach od *Światowej Organizacji Zdrowia* .

Po przeanalizowaniu tych danych naukowcy odkryli, że typowo „słoneczne" kraje, takie jak Hiszpania i Włochy (północne Włochy), mają zaskakująco wyższe wskaźniki niedoboru witaminy D. Kraje te doświadczyły również jednych z najwyższych wskaźników zakażeń COVID-19 i śmiertelności w Europie.

Z drugiej strony, kraje północnoeuropejskie, takie jak Norwegia, Finlandia i Szwecja, miały wyższe średnie stężenia witaminy D pomimo mniejszego nasłonecznienia ze względu na położenie geograficzne. Kraje te zgłosiły również niższe wskaźniki zakażeń COVID-19 i zgonów.

Sytuacja jest mniej więcej taka sama w innych krajach, takich jak Irlandia, Niemcy, Francja i Wielka Brytania. Podobnie jak kraje skandynawskie, te również zgłosiły niższe wskaźniki zakażeń COVID-19 i zgonów.

Ponadto naukowcy odkryli, że wyższe poziomy witaminy D częściej występują w krajach północnej Europy ze względu na suplementację. Ich ogólny poziom witaminy D brał się nie tylko

z tego, że spożywano suplementy czy wzbogaconą żywność, ale także ze spożywania naturalnych produktów.

Z drugiej strony, kraje o najwyższym wskaźniku niedoboru witaminy D spośród krajów objętych próbą nie miały takiej 'polityki wzbogacania żywności'. Wydaje się, że kraje te są również bardziej dotknięte COVID-19.

Biorąc pod uwagę te mocne dowody, naukowcy zasugerowali, że optymalizacja poziomu witaminy D zgodnie z zaleceniami dotyczącymi zdrowia publicznego może wzmocnić ogólną odpowiedź immunologiczną w celu lepszej ochrony przed COVID-19 i jego skutkami.

Naukowcy zauważyli również, że odpowiednia suplementacja i zwiększone spożycie pokarmów bogatych w witaminę D wydaje się być najlepszym sposobem działania, biorąc pod uwagę ograniczenia kwarantanny uniemożliwiające ludziom wychodzenie na miasto i opalanie się w celu wytworzenia witaminy D.

Niemniej jednak takie badania są wciąż trwają, powiedział główny autor Eamon Laird, badacz z *Trinity College w Dublinie*. On i jego koledzy uważają, że badania kliniczne są potrzebne, aby dostarczyć konkretnych dowodów. Odkrycia Lairda i jego zespołu zostały opublikowane w *Irish Medical Journal* .

Witamina D może znaczną odgrywać rolę jeśli chodzi o wskaźniki śmiertelności z powodu COVID-19

Jak dotąd większość dowodów potwierdzających zdolność witaminy D do ochrony przed COVID-19 pochodzi z badań obserwacyjnych, takich jak te przeprowadzone przez Lairda i jego współpracowników.

Badania takie jak te mogą nie dowodzić związku przyczynowego, ale dają wgląd w możliwe czynniki wpływające na ryzyko infekcji i wyniki kliniczne COVID-19, takie jak niedobory składników odżywczych.

Na przykład naukowcy z *Northwestern University* w Illinois odkryli, że poważny niedobór witaminy D i wysoka śmiertelność z powodu COVID-19 są silnie skorelowane po zbadaniu danych pacjentów z 10 krajów.

W szczególności pacjenci z COVID-19 z krajów o wyższej śmiertelności z powodu COVID-19, takich jak Włochy, Hiszpania i Wielka Brytania, mieli niższy poziom witaminy D niż pacjenci z innych krajów.

Ponadto naukowcy odkryli, że ciężka reakcja immunologiczna zwana burzą cytokin jest odpowiedzialna za poważne następstwa COVID-19, w tym śmierć, u pacjentów z niedoborem witaminy D.

Według głównego autora, Ali Daneshkhah, burza cytokin może poważnie uszkodzić płuca i zaostrzyć niewydolność oddechową u pacjentów. W kontekście infekcji wirusowej, burza cytokin jest wywoływana, gdy komórki odpornościowe wytwarzają nadmierne ilości białek zwanych cytokinami, aby zwalczyć infekcję.

W skrajnych przypadkach ta reakcja może spowodować niewydolność narządów. Dlatego Daneshkhah mówi, że nie jest zaskoczeniem, że burze cytokin wydają się być przyczyną większości zgonów z powodu COVID-19, a nie uszkodzenia płuc przez samego wirusa.

Współautor Daneshkhah, Vadim Backman, również uważa, że właśnie tutaj suplementacja witaminy D może stać się niezbędna. Jako składnik odżywczy wzmacniający odporność, witamina D może modulować odpowiedź immunologiczną na infekcję.

Dlatego posiadanie odpowiedniego poziomu witaminy D może chronić pacjentów z COVID-19 przed poważnymi komplikacjami z powodu nadaktywnej odpowiedzi immunologicznej, która prowadzi do śmierci.

Chociaż witamina D może nie zapobiec zarażeniu się wirusem, może pomóc zmniejszyć nasilenie powikłań i zapobiec śmierci

wśród pacjentów z COVID-19.

Z drugiej strony eksperci nie określili jeszcze odpowiedniej dawki witaminy D, która będzie najbardziej korzystna dla pacjentów z COVID-19 ze względu na brak badań klinicznych. W celu uniknięcia skutków toksyczności witaminy D należy przestrzegać odpowiedniej suplementacji opartej na przeważającej zalecanej dawce.

Podsumowując, badania te przyczyniają się do powstania materiału dowodowego potwierdzającego ochronne działanie witaminy D przed ciężkimi następstwami COVID-19

Źródła:

ScienceDaily.com 1

ScienceDaily.com 2

IMJ.ie

EurekAlert.org

Indyjska aplikacja do śledzeniea COVID ujawnia lokalizację obozów wojskowych

Ekspert GIS ostrzegł, że indyjska aplikacja do śledzenia COVID, Aarogya Setu, może udostępniać lokalizacje obozów wojskowych i może być wykorzystywana przez wrogów do inwigilacji i do śledzenia ruchów żołnierzy we wrażliwych obszarach, takich jak Pangong Tso w Ladakh.

Aarogya Setu ujawnia lokalizację obozów wojskowych

Wrażliwe informacje o rozmieszczeniu żołnierzy i ich ruchu w bazach wojskowych lub placówkach szpiegowskich wzdłuż granicy z Chinami mogły zostać naruszone przez aplikację mobilną Aarogya Setu do śledzenia COVID-19 w Indiach.

Aarogya Setu został zaprojektowany przez rząd w celu gromadzenia danych o lokalizacji i odniesienia ich do bazy danych testów COVID-19 należącej do Indian Council of Medical Research, aby ostrzec użytkownika, jeśli w pobliżu znajduje się zarażona osoba.

„Dzięki aplikacji można sprawdzić, czy żołnierz używający Arogya Setu znajduje się w konkretnym obozie, czy też wyjeżdża do innego obozu, czy jest przenoszony, czy coś w tym rodzaju. Przez stały pomiaru, można zobaczyć, jak wiele osób zostało przeniesionych z obozu i ile osób zjnaduje się w obozie w danej chwili" Raj Bhagat Palanichamy, niezależny system informacji geograficznej (GIS) – napisał Sputnik.

Ostrzegając władze, Raj podzielił się przykładem wykorzystania Arogya Setu do z grubsza wykrywania liczby osób korzystających z aplikacji (co może być zbieżne z liczbą żołnierzy) we wrażliwych obszarach, takich jak Pangong Tso, gdzie wojska Indii i Chin były zaangażowane w ostry konflikt od kwietnia tego roku.

„Dzięki fałszywej aplikacji GPS możesz przenieść swoją lokalizację w dowolne miejsce. Możesz po prostu wpisać cokolwiek do Wagah Border, Pangong Tso, Galwan Valley. To nic wielkiego. A potem możesz po prostu otworzyć aplikację Arogya Setu, która pokaże, ilu zwykłych ludzi (dotkniętych COVID)

jest tam itp.”- powiedział Raj, dodając, *„że chińscy agenci mogą nie uzyskać dokładnej liczby żołnierzy w określonej lokalizacji, ale „Będą wiedzieć, czy ludzie się poruszają i czy idą w jakim kierunku, w jakim czasie itp.”*

„Jeśli mówisz o miejscu, w którym znajduje się tylko baza wojskowa, nie jest wymagana żadna wiedza techniczna ani hakowanie. Ale jeśli chcesz dowiedzieć się czegoś o konkretnym budynku itp., trzeba trochę pokombinować ”- powiedział Raj Bhagat Sputnikowi.

Armia indyjska, wydając poradnik w kwietniu tego roku, poprosiła żołnierzy o zainstalowanie aplikacji Arogya Setu i włączenie usług lokalizacyjnych i bluetooth podczas odwiedzania miejsc publicznych, w ośrodkach izolacyjnych, powołując się na pomoc władzom cywilnym w związku z COVID-19 podczas podczas opuszczania kwater lub stacji wojskowych. W kwietniu personel armii został ostrzeżony, aby nie ujawniał swojej tożsamości służbowej, w tym rangi, stanowiska i listy kontaktów użytkowników podczas korzystania z takich aplikacji.

Jaki pogląd na Aarogya Setu ma Armia Indyjska?

Według wyższego rangą oficera armii, aplikacja Aarogya Setu mogłaby służyć do śledzenia lokalizacji żołnierzy, a żołnierze rozmieszczeni na wysuniętych posterunkach w ogóle nie powinni używać telefonów komórkowych.

„Zadbaliśmy o to, aby żołnierze rozmieszczeni na wysuniętych posterunkach nie korzystali z telefonów komórkowych. Komunikują się za pośrednictwem wojskowych urządzeń komunikacyjnych. Tak więc ich ruch ani lokalizacja nie zostaną ujawnione przeciwnikom za pośrednictwem aplikacji Aarogya Setu ”- powiedział w poniedziałek generał armii indyjskiej Sputnikowi.

Urzędnik armii indyjskiej przyznał jednak, że ruch z posterunków pokojowych i miejsc innych niż posterunki wysunięte może być śledzony. *„Nasze oddziały patrolujące*

wrażliwe obszary nie używają telefonów komórkowych” – stwierdził urzędnik.

Przejęty kod źródłowy Aarogya Setu

12 sierpnia firma zajmująca się bezpieczeństwem cybernetycznym z siedzibą w Bombaju opublikowała szczegółowy blog wyjaśniający, w jaki sposób odkryła kod źródłowy całej platformy Aarogya Setu, w tym jej infrastruktury zaplecza udostępnionej publicznie w Internecie.

W blogu stwierdzono, że przy otwartych danych dostępowych firma była w stanie „pobrać kod źródłowy witryny internetowej Aarogya Setu, portalu Swaraksha, wewnętrznych interfejsów API, usług internetowych i wewnętrznej analizy”.

Sprawa została skierowana do Indian Computer Emergency Response Team, który po cichu załatałł lukę.

Następnie rząd zagroził Shadow Map podjęciem kroków prawnych w związku z blogiem opisującym zagrożenia bezpieczeństwa Aarogya Setu.

Chociaż dużo uwagi poświęcono Aarogya Setu, kilka rządów stanowych uruchomiło własne aplikacje COVID-19. Badanie bezpieczeństwa tych aplikacji przez Centrum Internet and Society (CIS) okazało się, że większość z tych aplikacji nie mają konkretnej polityki prywatności.

Źródło:

BlacklistedNews.com