Upublicznianie w sieci materiałów o dziecku wiąże się z zagrożeniami. Eksperci radzą, jak im zapobiegać

Mimo informacji o kolejnych wyciekach danych oraz o inwigilacji relacjonowanie codziennego życia w mediach społecznościowych wciąż wydaje się nie tracić na popularności. Na stronie Centrum Informacji Konsumenckiej czytamy, że w Polsce ok. 40 proc. rodziców regularnie korzystających z internetu publikuje materiały dotyczące własnego dziecka. Z kolei według badań dr Anny Brosch z Wydziału Nauk Społecznych Uniwersytetu Śląskiego w Katowicach co czwarty rodzic permanentnie udostępnia w mediach społecznościowych informacje o swoich dzieciach, które traktowane jak „mikrocelebryci" dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Życie na wirtualnym świeczniku"

Zjawisko to nazywa się sharentingiem (ang. share – dzielić się i parenting – rodzicielstwo) i odnosi się do częstego upubliczniania informacji intymnych o dziecku, które naruszają jego prywatność i które mają zasięg publiczny, a więc mogą trafić do anonimowego odbiorcy. Mogą to być np. zdjęcia przedstawiające codzienne życie, ale i zdjęcia prześmiewcze, np. gdy dziecko zaśnie z nosem w talerzu.

Jak informują eksperci, ok. 23 proc. dzieci zaczyna istnieć

w sieci jeszcze przed fizycznym przyjściem na świat, ponieważ ich rodzice zamieszczają zdjęcia bądź nagrania z USG. Czasem nawet dzieci przebywające w łonie matki mają już profile w mediach społecznościowych.

Z poradnika „Sharenting i wizerunek dziecka w sieci" wydanego przez Akademię NASK dowiadujemy się, że spora część rodziców zamieszczających w sieci treści o swoim dziecku nie stosuje ograniczeń dotyczących wyświetlania materiałów i udostępnia je większym grupom osób.

Według badań przeprowadzonych przez dr Annę Brosch w 2018 roku w grupie 1036 rodziców dzieci w wieku przedszkolnym, co czwarty z nich nagminnie udostępnia takie informacje. „Nie jest to więc aż tak popularny proceder, ale na pewno zauważalny, bo jeżeli ktoś upowszechnia dziesiątki albo nawet setki zdjęć swoich dzieci, to odbiorcom wydaje się, że media społecznościowe są nimi zalane" – powiedziała dr Brosch.

Badaczka z Wydziału Nauk Społecznych Uniwersytetu Śląskiego zwraca uwagę, że sharentingiem zajmują się przeważnie matki.

„Dawniej np. w latach 70. XX wieku młode matki siadały przed blokiem na ławce, dzieci bawiły się w piaskownicy, a one rozmawiały o dzieciach. Teraz matki przeniosły się do sieci" – podkreśliła.

W ocenie dr Brosch matki udostępniają zdjęcia swoich dzieci z kilku powodów. Po pierwsze, żeby pokazać innym, jak dobrymi są matkami, że sobie doskonale radzą. Po drugie, poszukują wsparcia i akceptacji społecznej dla tego, co robią.

„Trzeci motyw związany jest z charakterystyczną dla naszych czasów modą na popularność. Chodzi o uzyskanie aprobaty społecznej poprzez lajki, co prowadzi do popularności. Wiele osób w sieci naśladuje innych – znanych tylko z tego, że są znani. Następnie oni sami chcą stać się takimi celebrytami. A że nie mają szansy dzięki sobie, to starają się to uzyskać

chociaż dzięki dziecku. Stąd np. te zdjęcia ośmieszające dzieci, które mają po prostu przykuwać uwagę" – tłumaczyła badaczka.

Brosch dodała, że ojcowie w dużo mniejszym stopniu ulegają sharentingowi, a jeżeli już, to najczęściej w sytuacji, gdy starają się o prawa do opieki nad dzieckiem.

Częściej kobiety ulegają sharentingowi niż mężczyźni. Robią to, by pokazać, że są dobrymi matkami, choć wiele z nich poszukuje również akceptacji i popularności. Zdjęcie ilustracyjne (MarieXMartin / Pixabay)

Stacey Steinberg, profesor z Levin College of Law na Uniwersytecie Florydy w Gainesville, podaje, że dla części rodziców sharenting jest rodzajem budowania więzi z rozproszoną rodziną, pomaga w dzieleniu się problemami i niweluje samotność. Badaczka podkreśla jednak, że należy pamiętać także o płynących z takiego działania zagrożeniach.

Jako obrończyni praw dzieci zaznaczyła, że dzieci powinny mieć prawo do decydowania, jakie informacje o nich chcą zamieścić

w sieci ich rodzice.

Nawet jeśli w danym przypadku publikowane treści nie narażą dziecka na różnego rodzaju represje, kradzież tożsamości czy może nie trafią na strony z pornografią dziecięcą, to pediatrzy są coraz bardziej świadomi znaczenia ochrony obecności dzieci w cyfrowej rzeczywistości i zwracają uwagę, by nie zapominać o prawie dziecka do prywatności.

Prywatność i „długa pamięć internetu”

„Każdy człowiek powinien mieć możliwość tworzenia własnej tożsamości i wizerunku, także w świecie cyfrowym” – podkreślają Anna Borkowska i Marta Witkowska, autorki poradnika „Sharenting i wizerunek dziecka w sieci”. Wszystkim niezależnie od wieku należy się prawo decydowania, jakie szczegóły z własnej prywatności chce ujawnić. Rodzice nagminnie dokumentujący w mediach społecznościowych życie własnych dzieci pozbawiają je możliwości wyboru, co i czy w ogóle chciałyby opowiedzieć o sobie w wirtualnym świecie.

Ponadto autorki poradnika dla rodziców o upublicznianiu wizerunku dziecka w sieci wymieniają jeszcze inne zagrożenia związane z sharentingiem.

Przypominają, że „internet ma długą pamięć” i w cyberprzestrzeni nic nie ginie, zwłaszcza że treści zyskujące dużą popularność dość szybko są rozpowszechniane, a zatem trudno je całkowicie usunąć.

„Internet nigdy nie zapomina, więc trudno przewidzieć konsekwencje tego procederu dla dzieci w przyszłości. W sieci nic nie ginie, a jeżeli wrzuci się do sieci jakieś zdjęcie, to zaczyna ono żyć własnym życiem. Nie mówiąc o skrajnych, ale jednak [mających miejsce], przypadkach kradzieży tożsamości w internecie czy pedofilach w sieci” – mówi dr Brosch.

Utrata kontroli

Na przykład w 2015 roku w Australii wykazano, że około połowa z 45 mln zdjęć znajdujących się na stronie z pornografią dziecięcą pochodziła bezpośrednio z mediów społecznościowych i były to przeważnie niewinne zdjęcia z codziennej scenerii, które pojawiały się w kontekście niestosownych komentarzy.

Dlatego eksperci podkreślają, by pamiętać, że nad fotografiami wrzuconymi do sieci, przestaje się mieć pełną kontrolę i nie można być pewnym, kto i w jaki sposób je wykorzysta. Mogą zostać bezprawnie użyte w celach majątkowych bądź przestępczych.

Specjaliści ostrzegają, że „media społecznościowe są bardzo często terenem poszukiwań dla pedofilów, którzy nagminnie pobierają z nich zdjęcia dzieci i handlują nimi na zamkniętych forach internetowych".

Przestępstwo posługiwania się skradzionym wizerunkiem dziecka w celu realizowania swoich fantazji nazywane jest cyfrowym kidnapingiem (ang. baby role play).

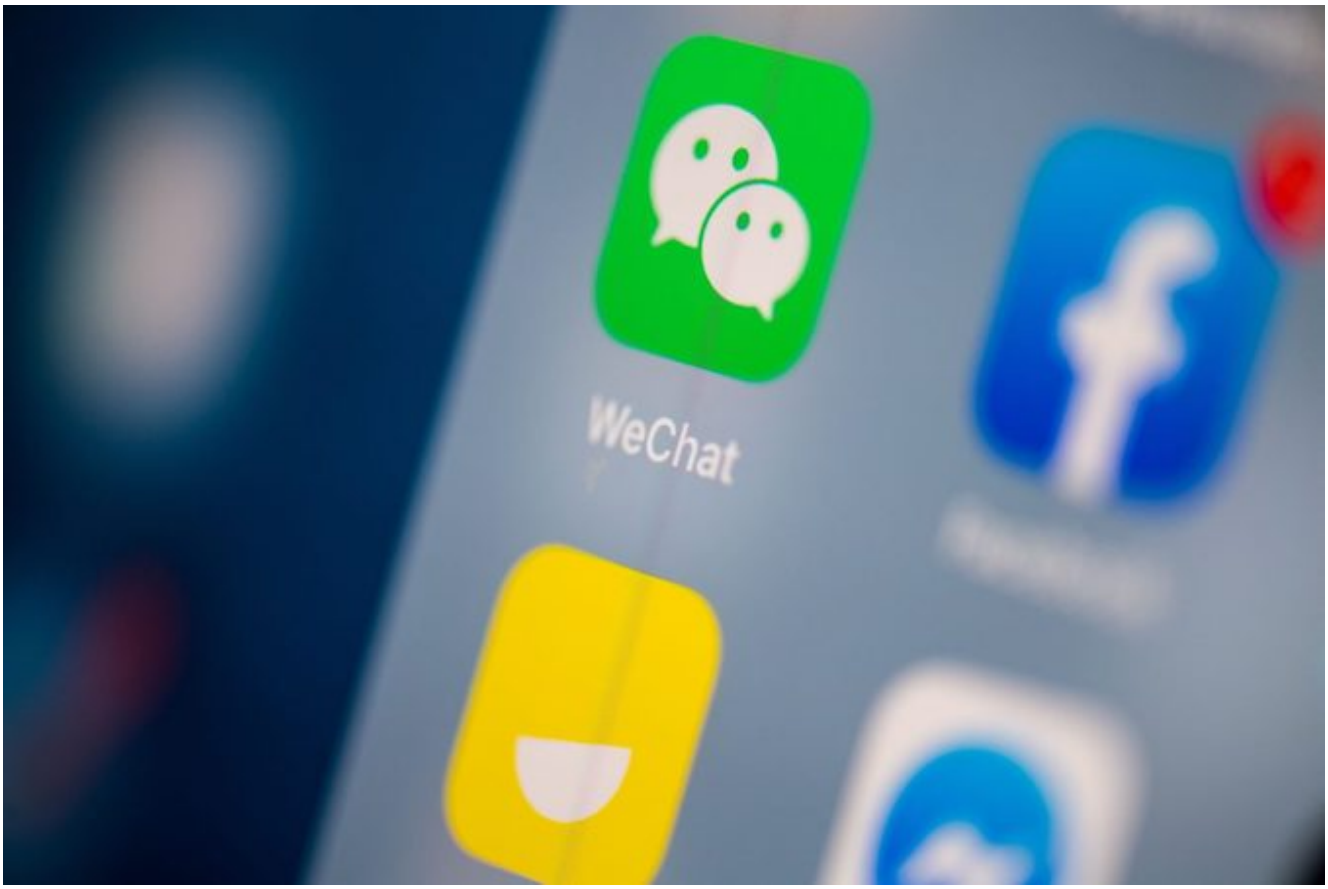
Nie powinniśmy też narażać dzieci na cyberprzemoc. Asumptem do tego może być publikowanie w naszej opinii zabawnych zdjęć dziecka, które jednak w szerszej perspektywie mogą zostać odebrane jako kompromitujące. To może spowodować falę hejtu i agresji ze strony zarówno nieznajomych internautów, jak i rówieśników dziecka oraz wpłynąć na jego samoocenę.

Wykorzystywanie danych osobowych

Pozostaje też kwestia udostępniania danych osobowych, które „wymieniamy" za możliwość korzystania z profilu w mediach społecznościowych. Stanowią one źródło informacji m.in. dla firm marketingowych.

Co więcej, eksperci ds. Chin, a także politycy od lat alarmują, by nie korzystać z chińskich technologii, m.in. TikToka czy WeChata, oraz innych pozornie niegroźnych

narzędzi, które gromadzą dane na temat użytkowników, a także pozyskują w nielegalny sposób poufne informacje i wrażliwe dane z różnych instytucji. Gdy takie informacje znajdą się w rękach reżimu komunistycznego, mogą zagrażać bezpieczeństwu krajów oraz ich mieszkańców.



Ilustracja demonstrująca logo chińskiego komunikatora WeChat wyświetlonego na tablecie, 24.07.2019 r. (Martin Bureau/AFP/Getty Images)

Komunistycznej Partii Chin do zbierania danych służą np. platformy społecznościowe, komunikatory, programy do obróbki i „ulepszania" zdjęć lub aplikacje usprawniające pisanie maili.

Władze ChRL wykorzystują „systemy big data do inwigilacji – zwłaszcza w celu sprawdzenia, czy ktoś ma opinie sprzeczne z prezentowanymi przez chiński reżim. Jednym ze sposobów jest analizowanie zakupów w sklepach internetowych" – powiedział profesor nauk politycznych dr Titus C. Chen z Narodowego Uniwersytetu Sun Yat-sena na Tajwanie.

Niemal wszechobecny monitoring w Chinach oraz nadzorowanie aktywności w internecie używane są do tzw. systemu oceny (ang. social credit system). Według niego każdemu obywatelowi są przyznawane punkty „społecznej wiarygodności". Ludziom mogą zostać odjęte punkty z ich wyniku oceny społecznej, jeśli popełnią czyn uznawany przez KPCh za niepożądany, jak np. przejście przez ulicę w miejscu niedozwolonym. Osoby z niskimi wynikami oceny społecznej są uważane za „niegodne zaufania", a tym samym pozbawiane dostępu do usług i możliwości. Może chodzić np. o zakaz podróżowania samolotem lub uczęszczania do szkół.

System służy do prześladowania m.in. zwolenników duchowej praktyki Falun Gong, Ujgurów i innych grup, które KPCh próbuje zniszczyć.

Pojawiające się co jakiś czas informacje o wycieku danych pokazują, że KPCh infiltruje nie tylko obywateli ChRL, ale uważnie obserwuje osoby na Zachodzie.

Konsekwencje

Zdaniem dr Anny Brosch sharenting sprawia, że dzieci zaczynają być traktowane jak „mikrocelebryci", którzy dorastają w przeświadczeniu, że dzielenie się szczegółami z prywatnego życia jest naturalną praktyką.

„Można więc przypuszczać, bo to wymaga jeszcze badań, że gdy w przyszłości sami zostaną rodzicami, będą jeszcze bardziej otwarci i skłonni do samoujawniania. Ale z drugiej strony, to już się dzieje, nastolatkowie proszą rodziców o usunięcie zdjęć i informacji o sobie; za granicą były nawet przypadki sądowych rozpraw" – mówiła dr Brosch.

Badania dr Brosch wykazują, że sharenting się zmienia.

„Coraz mniej już jest zasypywania całymi seriami przypadkowych zdjęć. Teraz są one przemyślane. Wzrasta jednak nastawienie rodziców na zachowania celebryckie i na zyski – im więcej

lajków, tym większa popularność i być może możliwość zarabiania pieniędzy z umów na produkty lokowane. W takich przypadkach mogą to być nawet kompromitujące filmy, ale liczy się zasięg" – zauważyła.

Znawcy przedmiotu doradzają zastanowienie się, jakie treści o naszych pociechach wrzucamy do sieci i jakie to może mieć konsekwencje w przyszłości. Jeśli decydujemy się na publikację, róbmy to odpowiedzialnie. Pamiętajmy, że nawet najlepsze zabezpieczenia nie dadzą nam pełnej ochrony przed niepożądaną kradzieżą wizerunku.

Dbajmy też o to, by nie narazić dzieci na ostracyzm i uczmy je świadomego podejścia do upubliczniania informacji w cyberprzestrzeni.

Źródła: PAP, Centrum Informacji Konsumenckiej, Akademia NASK, NPR.

Google śledzi użytkowników Chrome nawet w trybie „incognito"

Jeśli używasz przeglądarki Google Chrome do surfowania po sieci i robisz to „incognito", co ma oznaczać przeglądanie prywatne, powinieneś wiedzieć, że gigant z Doliny Krzemowej

nadal potajemnie śledzi twoją aktywność w sieci.

Firma Alphabet Inc. twierdzi, że aktywacja trybu „stealth" w Chrome oznacza po prostu, że firma nie „zapamięta Twojej aktywności". Nie oznacza to, że Google nie jest w stanie zobaczyć, które strony odwiedzasz i jak często je odwiedzasz, co dla niektórych może być zaskoczeniem.

Sędzia okręgowy USA Lucy Koh, znana z tego, że wzięła się za Big Tech, które jest winne zbrodni przeciwko ludzkości, odpowiedziała na pozew zbiorowy przeciwko Google, mówiąc, że jest „zaniepokojona" praktykami gromadzenia danych przez międzynarodową korporację, które w najlepszym przypadku są zwodnicze.

Pozew domaga się 5000 dolarów odszkodowania za każdego z milionów użytkowników Chrome, których prywatność została naruszona od czerwca 2016 roku. Koh mówi, że uważa za „niezwykłe" to, że Google dokłada „dodatkowego wysiłku" w celu zebrania takich danych, jeśli rzekomo tego nie robi aby profilować użytkowników i kierować do nich reklamy.

Firma Google jest i była uwikłana w liczne procesy sądowe dotyczące jej praktyk monopolistycznych, w tym naruszania prywatności w reklamach cyfrowych i wyszukiwaniu online. W jednym z nich Koh skutecznie zmusiła Google do ujawnienia skanowania prywatnych wiadomości e-mail w celu tworzenia profili i kierowania reklam.

W tym przypadku Google jest oskarżany o osadzanie kodu w witrynach internetowych, które wykorzystują jej usługi analityczne i reklamowe do pobierania danych z rzekomo prywatnej historii przeglądania użytkowników i przekazywania ich na serwery Google w celu przetworzenia.

Google sprawia wrażenie, jakby tryb przeglądania prywatnego zapewniał użytkownikom większą kontrolę nad ich danymi, mówi prawniczka Amanda Bonn, ale w rzeczywistości „Google twierdzi, że w zasadzie niewiele można zrobić, aby uniemożliwić nam

gromadzenie Twoich danych, i właśnie to powinieneś założyć”

Google to zło; przestań używać ich produkty

Andrew Shapiro, prawnik Google, twierdzi, że polityka prywatności jego klienta „wyraźnie ujawnia” fakt, że podczas korzystania z produktu Google prawie nic nie jest prywatne.

„Gromadzenie danych, o którym mowa, zostało ujawnione” – mówi.

Stephen Broome, inny prawnik Google, mówi, że strony internetowe, które zawierają umowę z Google na korzystanie z jej narzędzi analitycznych lub innych usług, doskonale znają praktyki gromadzenia danych jego klientów i nie jest to tajemnicą.

Broome próbował bagatelizować obawy powodów, a także sądu dotyczące prywatności, wskazując, że własna strona internetowa federalnego sądu korzysta z usług Google. Ta taktyka przyniosła jednak odwrotny skutek, gdy sędzia zażądał wyjaśnienia „co dokładnie robi Google”, wyrażając jednocześnie obawy, że osoby odwiedzające witrynę sądu nieświadomie ujawniają Google prywatne informacje.

„Chcę oświadczenia od Google na temat tego, jakie informacje gromadzą o użytkownikach witryny sądu i do czego są one wykorzystywane” – powiedziała Koh prawnikom Google.

Wniosek z tego wszystkiego jest taki, że Google nie można i nie powinno się ufać. Wszystko, co robi, ma na celu zarabianie pieniędzy, przejęcie władzy, eliminację praw ludzi i ostatecznie osiągnięcie dominacji nad światem.

„Ponadto Google i Alphabet ukradły kod Oracle, więc cała ich działalność opiera się na tej kradzieży” – zauważył jeden z naszych komentatorów o kolejnej króliczej dziurze Google.

„Sprawa jest w tej chwili w Sądzie Najwyższym i wkrótce zostanie rozpatrzona. Naprawdę łatwo to udowodnić, Google jest skończone. Nawet przestępcy w Sądzie Najwyższym nie mogą

pozwolić sobie na to. To zbyt oczywiste”.

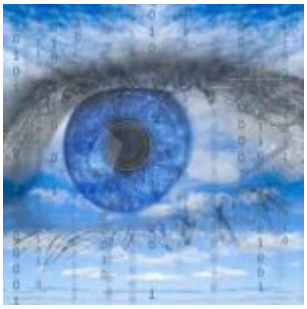
Inny komentator zgodził się z tym, dodając, że „dni Google są policzone”, ponieważ „nigdy nie nauczą się, że wahadło może wychylać się tylko daleko w jednym kierunku, i musi wrócić”.

Źródła tego artykułu obejmują:

BNNBloomberg.ca

NaturalNews.com

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

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

Nowozelandzkie „Obozy" Kwarantanny COVID-19 to koniec wolności osobistej

Naród wyspiarski na Pacyfiku ma 25 zgonów z powodu koronawirusa na prawie pięć milionów mieszkańców…

Starszy współpracownik Hoover Institution, Victor Davis Hanson, potępił

nowozelandzką instytucję „obozów ” kwarantanny koronawirusa we wtorkowym „The Ingraham Angle”.

Premier Jacinda Ardern z centrolewicowej Partii Pracy w Nowej Zelandii ogłosiła w filmie, że jeśli ludzie wysłani do obozu odmówią poddania się badaniom, będą musieli pozostać jeszcze dwa tygodnie po początkowym dwutygodniowym pobycie.

Ardern nazwała ostrzeżenie „całkiem dobrą zachętą” do wykonania testu na obecność COVID-19.

> *„Albo wykonasz test i upewnisz się, że jesteś czysty, albo zatrzymamy cię w ośrodku na dłużej” – powiedziała.*

> *„Myślę więc, że większość ludzi patrzy na to i mówi: „Podejdę do testu”".*

Hanson powiedział gospodarzowi Laurze Ingraham, że takie drakońskie środki, jak rozkazy Ardern nie mają sensu, biorąc pod uwagę, jak niewielki wpływ tzw. pandemii wywarła na wyspiarski kraj.

> *„Mają 5-milionowy naród” – wyjaśnił Hanson.*

> *„Stracili, tragicznie, ale stracili 25 osób. To zdumiewająco niska liczba, jeśli chodzi o pozbycie się wolności osobistej”.*

„Tutaj, w Stanach Zjednoczonych, czy to [gubernator Kalifornii] Gavin Newsom, Michelle Obama czy Joe Biden, wszyscy powiedzieli, że jest to okazja, aby nie odpuszczać” – dodał.

W dalszej części tego segmentu Ingraham zacytował doniesienie niemieckich mediów, że Parlament Europejski i Komisja Europejska używają kamer termowizyjnych wyprodukowanych w Chinach, aby zapobiec rozprzestrzenianiu się COVID-19.

W raporcie DW.com zauważono, że firma produkująca kamery jest również oskarżana o dostarczanie technologii wykorzystywanej przez Pekin do patrolowania i nadzorowania muzułmańskich obozów internowania w prowincji Xinjiang.

> *„Czy tego typu scenariusze będziemy musieli stawić czoła pod administracją Bidena?” – zapytała Hansona.*

> *„Tak, to przerażające” – odpowiedział.*

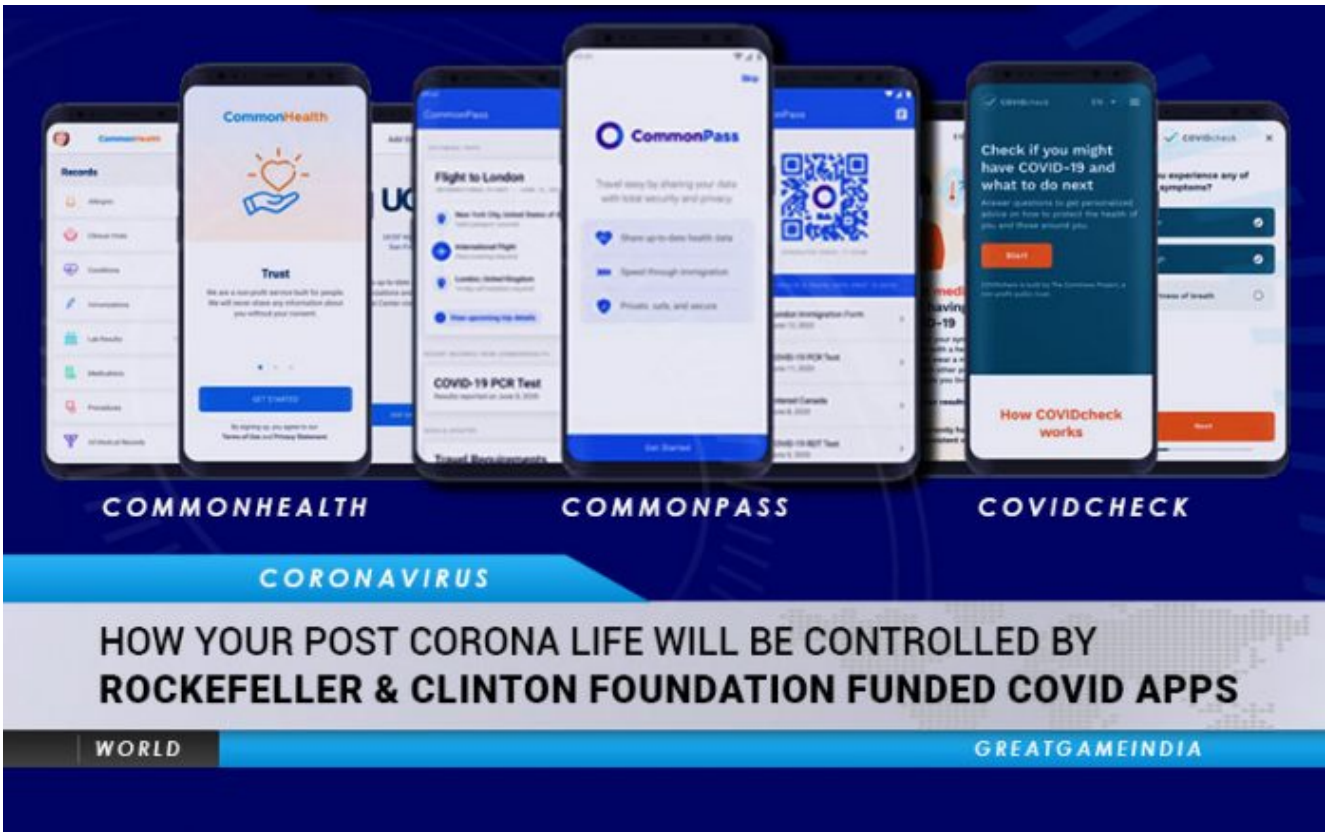
„Wirus zaczął się w Chinach, rozprzestrzenił się z Chin, a teraz Chiny oferują Zachodowi metodologię i technologię faszyzmu, aby rzekomo wyleczyć to, co zaczęło”.

Źródło:

humansarefree.com

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.

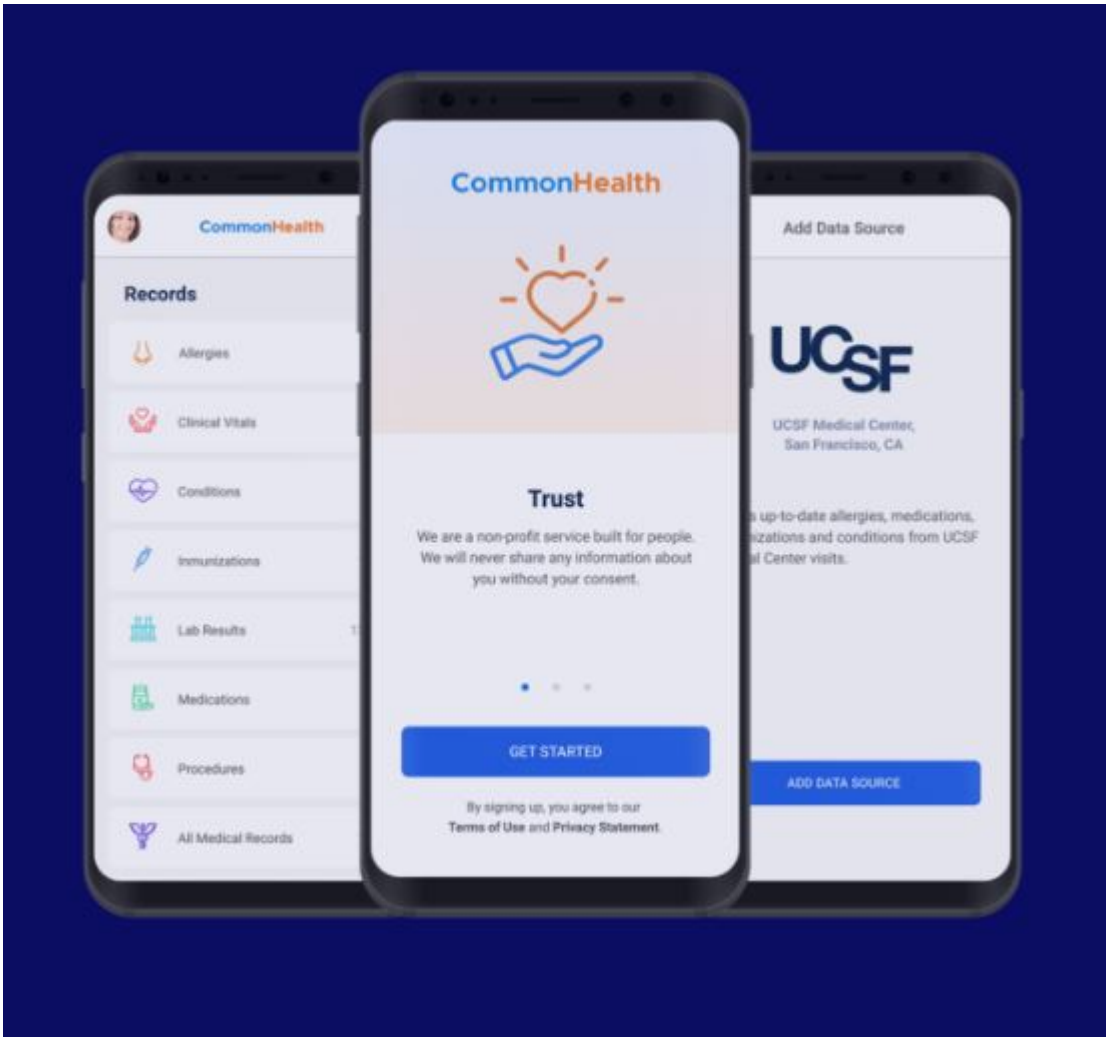
Na stronie www The Commons Project tak opisują swoją rolę:

*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

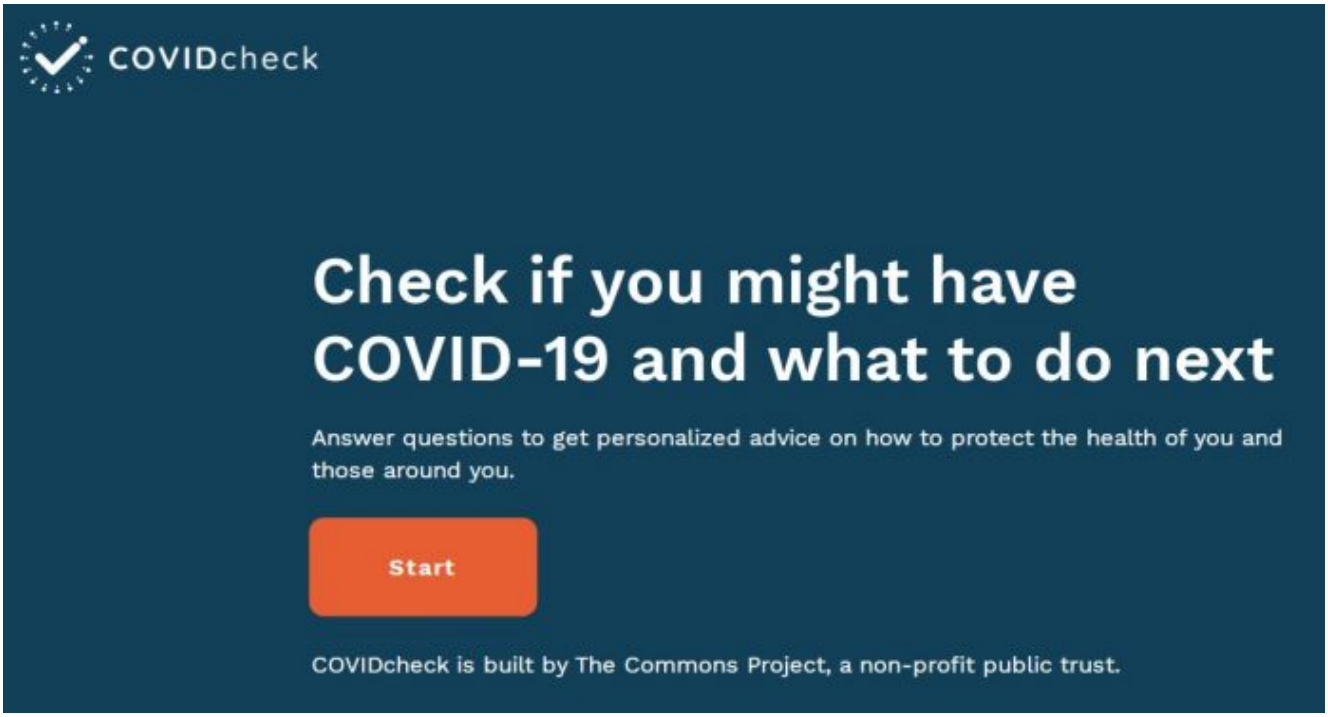
CommonHealth będzie gromadzić i zarządzać Twoimi osobistymi danymi zdrowotnymi oraz udostępniać je służbie zdrowia, organizacjom i innym aplikacjom. Celem CommonHealth jest rozszerzenie modelu przenoszenia danych zdrowotnych i współdziałania, którego pionierem jest Apple Health, na 73% ludzi na całym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

Facebook oskarżony o podglądanie przez kamery użytkowników Instagrama

Firma Facebook Inc. ponownie została pozwana za rzekome szpiegowanie użytkowników Instagrama, tym razem poprzez nieautoryzowane użycie ich aparatów w telefonach komórkowych.

Pozew pochodzi z lipcowych doniesień mediów, że aplikacja do udostępniania zdjęć wydawała się uzyskiwać dostęp do aparatów

iPhone’a, nawet jeśli nie były one aktywnie używane.

Facebook zaprzeczył zgłoszeniom i obwinia błąd, który, jak twierdzą, został poprawiony, a wywoływał coś, co opisali jako fałszywe powiadomienia, że Instagram uzyskuje dostęp do aparatów iPhone’a.

W skardze złożonej w czwartek w sądzie federalnym w San Francisco, użytkownik Instagrama z New Jersey, Brittany Conditi, twierdzi, że aplikacja aparatu używa aparatu celowo i ma na celu gromadzenie „lukratywnych i wartościowych danych o użytkownikach, do których w innym przypadku nie miałaby dostępu.”

Dzięki „pozyskiwaniu niezwykle prywatnych i intymnych danych osobowych swoich użytkowników, w tym w zaciszu własnego domu”, Instagram i Facebook mogą gromadzić „cenne spostrzeżenia i badania rynkowe”, zgodnie z treścią skargi.

Facebook odmówił komentarza.

W pozwie wniesionym w zeszłym miesiącu, Facebook został oskarżony o wykorzystywanie technologii rozpoznawania twarzy do nielegalnego gromadzenia danych biometrycznych ponad 100 milionów użytkowników Instagrama. Facebook zaprzeczył twierdzeniu i powiedział, że Instagram nie używa technologii rozpoznawania twarzy.

Sprawa to Conditi przeciwko Instagram, LLC, 20-cv-06534, Sąd Okręgowy Stanów Zjednoczonych, Północny Dystrykt Kalifornii (San Francisco).

Źródło:

bloomberg.com

W USA od niedzieli dostęp do chińskich aplikacji TikTok i WeChat będzie zablokowany

Dostęp do aplikacji TikTok i WeChat, należących do chińskich firm ByteDance i Tencent, od niedzieli o północy zostanie zablokowany w Stanach Zjednoczonych. Administracja prezydenta Donalda Trumpa powołuje się na obawy dotyczące bezpieczeństwa narodowego.

Zgodnie z nowymi zasadami określonymi przez Departament Handlu USA sklepy z aplikacjami będą miały zakaz dystrybuowania i obsługi TikToka i WeChata od niedzieli. Aktualni użytkownicy TikToka nadal będą mogli korzystać z aplikacji do 12 listopada, jednak od północy w niedzielę nie uzyskają dostępu do aktualizacji.

WeChat już w niedzielę zostanie całkowicie zablokowany w Stanach Zjednoczonych.

„TikTok w podstawowej formie pozostanie niezmieniony do 12 listopada" – powiedział w piątek dla Fox Business sekretarz ds. handlu Wilbur Ross. „Jeśli do 12 listopada nie doszłoby do zawarcia umowy zgodnie ze starym rozporządzeniem, z praktycznego punktu widzenia TikTok również zostałby wyłączony" – dodał, odnosząc się do rozporządzenia wykonawczego prezydenta Trumpa, nakazującego ByteDance, chińskiej firmie macierzystej, do której należy TikTok, zbycie wszystkich jej amerykańskich aktywów do 12 listopada.

Jak podano w komunikacie Departamentu Handlu: „Komunistyczna Partia Chin (KPCh) zademonstrowała możliwości i motywy używania tych aplikacji, aby zagrozić bezpieczeństwu narodowemu, polityce zagranicznej i gospodarce Stanów Zjednoczonych. Dzisiejsze ogłoszone zakazy, łącznie, chronią użytkowników w USA, eliminując dostęp do tych aplikacji i znacznie zmniejszając ich funkcjonalność".

Decyzja Departamentu Handlu to odpowiedź na rozporządzenia wykonawcze prezydenta Donalda Trumpa, nakazujące zablokowanie części operacji tych aplikacji, które uznał on za zagrożenie dla bezpieczeństwa narodowego USA. Ma to związek z gromadzeniem danych przez aplikacje należące do chińskich firm ByteDance (TikTok) i Tencent (WeChat).

TikTok to aplikacja umożliwiająca dzielenie się krótkimi filmami wideo, która zyskała wielką popularność wśród młodych ludzi w USA i na świecie. W Stanach Zjednoczonych ma 100 mln użytkowników.

WeChat to komunikator, sieć społecznościowa, a także system mobilnych płatności, posiadający ponad miliard użytkowników w Chinach i innych krajach Azji. W USA korzysta z niego 19 mln użytkowników.

Wśród użytkowników TikToka są również politycy. Prezydent Francji Emmanuel Macron w krótkim filmie gratulował uczniom szkół średnich matury. W Polsce pod koniec marca prezydent Andrzej Duda rozpoczął korzystanie z TikToka od zaproszenia uczniów do wzięcia udziału w turnieju organizowanym przez Ministerstwo Cyfryzacji, jednak później zaprzestał używania komunikatora. W sobotę prezes PiS Jarosław Kaczyński na TikToku apelował o poparcie dla projektu ustawy dotyczącej ochrony zwierząt, m.in. zakazu hodowli zwierząt futerkowych.

TikTok i WeChat a prawa człowieka

Istnieją jednak istotne różnice pomiędzy TikTokiem i WeChatem a innymi aplikacjami społecznościowymi, z których korzystają

internauci i dzięki którym można docierać z informacjami do milionów ludzi.

TikTok, oprócz gromadzenia danych użytkowników w tak dużym stopniu, że jeden z ekspertów nazwał komunikator „atrakcyjną bazą danych" dla chińskiego reżimu komunistycznego, cenzuruje publikowane treści. Konto studenta, który po przyjęciu przez Hongkong ustawy o ochronie chińskiego hymnu w akcie sprzeciwu udostępnił nagranie, w satyryczny sposób ukazujące chińskich urzędników i niewłaściwe obchodzenie się z pandemią przez KPCh, po niespełna dobie zostało usunięte.

Na TikToku, który działa według wskazań KPCh, użytkownik może nie znaleźć treści niezgodnych z polityką władz komunistycznych. We wrześniu 2019 roku „The Guardian" informował, że TikTok poinstruował swoich moderatorów, by cenzurowali filmy wideo, które wspominają tematy uważane przez chiński reżim za tabu. Do tematów niewygodnych dla KPCh należą masakra na placu Tiananmen i Falun Gong, praktyka duchowa składająca się z pięciu ćwiczeń medytacyjnych, oparta na naukach moralnych skupionych wokół zasad Prawdy, Życzliwości i Cierpliwości, która od 1999 roku jest brutalnie prześladowana w Chinach. Najpotworniejszym przejawem represji trwających już dwie dekady jest grabież organów od żywych ludzi usankcjonowana przez państwo.

Informacje o moderacji na TikToku zostały podane na podstawie ujawnionych dokumentów, zawierających szczegółowe wytyczne na ten temat. TikTok przekazał wówczas w oświadczeniu, że te zasady zostały zmienione w maju 2019 roku i nie są już używane.

W rozporządzeniu wykonawczym prezydenta Donalda Trumpa dotyczącym TikToka wymieniono również cenzurę treści dotyczących protestów w Hongkongu i represji wobec Ujgurów w prowincji Xinjiang. Według szacunków ponad milion Ujgurów zostało umieszczonych w obozach koncentracyjnych, są także zmuszani do pracy przymusowej.

Z kolei według raportu Citizen Lab przesyłanie wiadomości na WeChacie nie tylko naraża użytkownika na cenzurę, lecz także umożliwia zaostrzanie systemu cenzury wobec użytkowników w Chinach, ponieważ reżim w ten sposób dopracowuje algorytm wychwytujący treści w tym kraju zakazane.

Jak ostrzegają eksperci, każda chińska firma znajduje się pod kontrolą reżimu komunistycznego, a wszelkie dane, do których takie przedsiębiorstwa mają dostęp, pozostają do dyspozycji KPCh.

Źródła:

Trump Administration Banning Access to Chinese Apps WeChat and TikTok

U.S. Department of Commerce

PAP

Chiński reżim „przewodzi światu w prześladowaniu" grup wyznaniowych – mówi ambasador USA Sam Brownback

Chiński reżim komunistyczny przez lata „udoskonalał" swój mechanizm represji wobec grup wyznaniowych, a teraz stara się eksportować swój autorytarny model na cały świat, ostrzegł ambasador USA ds. międzynarodowych swobód religijnych Sam Brownback.

Reżim reklamuje się jako światowy lider, „jednakże światu przewodzi on w prześladowaniach – globalne przywództwo objął w prześladowaniach" – powiedział Brownback w niedawnym wywiadzie do programu „American Thought Leaders" w „The Epoch Times".

Powiedział, że kolejne kampanie prześladowań wobec praktykujących Falun Gong, buddystów tybetańskich, chrześcijan, a ostatnio ujgurskich muzułmanów w regionie Xinjiang, prowadzone przez Komunistyczną Partię Chin (KPCh) umożliwiły jej dopracowanie metod i technologii wykorzystywanych do inwigilacji i ucisku.

„Naprawdę ucisk w przyszłości widzimy jako mniejszą liczbę osób w obozach koncentracyjnych i większą liczbę osób kontrolowanych w społeczeństwie z 24-godzinnymi systemami nadzoru ludzi i ograniczaniem tego, co mogą robić w danym społeczeństwie" – dodał.

Ambasador powiedział, że niedawne sankcje administracji Trumpa przeciwko chińskim urzędnikom i grupie o paramilitarnej budowie zaangażowanej w łamanie praw człowieka w Xinjiang pokazują, że Stany Zjednoczone poważnie myślą o wysłaniu Pekinowi wiadomości. Również Departament Handlu USA umieścił na czarnej liście ponad 30 chińskich firm i podmiotów rządowych z powodu ich roli we wspomaganiu represji Ujgurów w tamtym regionie.

Brownback wyraził zaniepokojenie, iż KPCh zamierza wyeksportować swój model zaawansowanych technologicznie represji.

„Zamierzają zacząć wprowadzać na rynek i sprzedawać tego

rodzaju autorytarne systemy kontroli innym autorytarnym reżimom na całym świecie, które […] starają się kontrolować swoją populację za pomocą tych zaawansowanych technologii" – powiedział.

Ambasador powiedział, że ateistyczna KPCh, od chwili swojego powstania, jest przeciwna wierze.

„Nie ma w niej miejsca na wiarę w wyższy autorytet moralny" – powiedział. „Najwyższym autorytetem moralnym jest partia komunistyczna".

Brownback powiedział, że reżim może jawić się jako oszczerczy i prześladujący mniejszości, ale jego taktyka na tym się nie kończy.

„Tak było w całej historii. Jeśli nie przeciwstawisz się zbirom, to po prostu przyjdą" – powiedział.

Dla przykładu, świat przez lata przymykał oko na zarzuty, że KPCh siłą usuwa narządy uwięzionym praktykującym Falun Gong, by sprzedawać je na rynku transplantacyjnym, powiedział Brownback. A jednak „były tam dowody poszlakowe" (ang. circumstantial evidence), powiedział, dodając, że teraz istnieją wiarygodne instytucje, które twierdzą, że [w ChRL] ma miejsce usankcjonowana przez państwo grabież organów.

W 2019 roku niezależny trybunał społeczny (Niezależny Trybunał w sprawie Grabieży Organów od Więźniów Sumienia w Chinach, ang. Independent Tribunal into Forced Organ Harvesting from Prisoners of Conscience in China, obradujący w Londynie, pod przewodnictwem Sir Geoffreya Nice'a QC, który kierował oskarżeniem byłego prezydenta Jugosławii Slobodana Miloševicia podczas posiedzeń Międzynarodowego Trybunału Karnego dla byłej Jugosławii w Hadze – przyp. redakcji), po całorocznym śledztwie, stwierdził, że grabież organów miała miejsce w Chinach „na znamienną skalę" i nadal trwa. Okazało się, że głównym źródłem narządów byli uwięzieni praktykujący Falun Gong.

„Po prostu wyobraź to sobie, że zabierasz i prześladujesz danego człowieka. Zamierzasz zabić, a następnie zabrać organy, aby je sprzedać. Po prostu to, co się dzieje, jest przerażające” – powiedział Brownback.

Źródło:

theepochtimes.com