

# **Elektroniczna smycz dla mieszkańców Unii. „Europejski portfel tożsamości cyfrowej” da Brukseli pełną kontrolę nad obywatelami Wspólnoty**



Parlament Europejski i Rada Unii Europejskiej porozumiały się w sprawie utworzenia „europejskich portfeli tożsamości cyfrowej” (eID), centralnego, cyfrowego systemu identyfikacji wszystkich Europejczyków. To aplikacja, która ma służyć do załatwiania spraw urzędowych przez Internet na poziomie Unii, ale też korzystania z usług online i samej sieci. W portfelu mają się znaleźć cyfrowe wersje dokumentów obywateli, a także cyfrowe pieniądze. Wielu ekspertów i przedsiębiorców ostrzega jednak przed potencjalnymi nadużyciami na wielką skalę. Portfel da władcom Europy możliwość pozbawiania obywateli ich fundamentalnych praw i praktycznie noeograniczonej kontroli nad nimi. To narzędzie do zaprowadzenia usmiechniętej, liberalnej tyranii.

Zgodnie z nowym prawem UE ma oferować obywatelom tzw. „portfele cyfrowe” – początkowo na zasadzie dobrowolności, które będą zawierać cyfrowe wersje ich dowodów osobistych, praw jazdy, dyplomów, dokumentacji medycznej, informacji o kontaktach etc. Ma to ułatwić załatwianie spraw urzędowych, korzystanie z usług online na terenie Unii, jak też poświadczania tożsamości i uznawanie dokumentów. W skrócie:

w Portugalii nie będzie problemu z uzyskaniem i potwierdzeniem dokumentacji medycznej polskiego obywatela gdy ten znajdzie się w tamtejszym szpitalu. Podobnie ubezpieczeń, zezwoleń etc.

*Wszyscy obywatele UE będą mieli możliwość posiadania unijnego portfela tożsamości cyfrowej, umożliwiającego dostęp do publicznych i prywatnych usług online przy pełnym bezpieczeństwie i ochronie danych osobowych w całej Europie*

napisała Komisja Europejska w oświadczeniu.

Zaś Nadia Calvino hiszpańska wicepremier i minister cyfryzacji, która przewodzi teraz hiszpańskiej prezydencji w Unii oświadczyła pompatycznie:

*Zatwierdzając europejskie rozporządzenie w sprawie tożsamości cyfrowej, podejmujemy zasadniczy krok, aby obywatele mogli mieć niepowtarzalną i bezpieczną europejską tożsamość cyfrową. Jest to kluczowy postęp, dzięki któremu Unia Europejska może stać się światowym punktem odniesienia w dziedzinie cyfrowej, chroniącym nasze demokratyczne prawa i wartości.*

Oczywiście to unijny bełkot. Niby co ma wspólnego cyfrowe potwierdzanie tożsamości etc z demokracją i jakimiś tam wartościami europejskimi. Jeśli już to tylko dlatego, że im zagraża na co wskazuje 504 naukowców, ekspertów ds. prywatności i cyberbezpieczeństwa z 39 krajów, którzy podpisali wspólny list ostrzegający przed pułapkami, owego portfela i zagrożeniami jakie się z nim wiążą dla naszego bezpieczeństwa w sieci i wolności. W Polsce praktycznie nikogo to nie interesuje. Pod listem znalazł się podpis tylko jednego przedstawiciela naszego kraju – prof. Mirosława Kutylowskiego z PAN. [Tutaj jest link do listu protestacyjnego](#)

By pojąć istotę zagrożeń warto cofnąć się kilka lat, gdy prace nad cyfrową tożsamością zostały bardzo przyspieszone. Wiązało

się to z pandemią i wprowadzaniem paszportu covidowego. W istocie chodziło o szybką identyfikację tych, którzy nie zaszczepili się, więc zostali pozbawieni swych podstawowych praw – jak choćby możliwości przemieszczania się, podróży. Tych którzy nie mieli elektronicznych zaświadczeń o tym, że dobrowolnie poddali się przymusowemu szczepieniu w praktyce można było trzymać w gettach dla sanitarnie podejrzanych, czy nieprawidłowych. Nowy, projektowany portfel cyfrowy daje nieskończenie większe możliwości pozbawiania ludzi praw i zniewalania ich.

Już w pierwszej zalecie owego portfela – w tym, że wszystkie dokumenty będą w jednym miejscu, dostępne za pomocą jednego przycisku – jak zachwalają eurokraci, tkwi jedno z największych zagrożeń. Oznacza to bowiem, że jednym przyciskiem można nas też wszystkich dokumentów pozbawić. Póki są one rozproszone znacznie trudniej jest to zrobić. Ćwiczył to już w Kanadzie reżim Trudeau, który pozbawiał niezgadających się na covidowy zamordyzm dostępu do kont, czyli pieniędzy, ale też unieważniał ubezpieczenia w kierowcom ciężarówek, którzy utworzyli wielki konwój protestacyjny.

Kontroli nad obywatelami nie sprawowałyby nawet rządy poszczególnych państw, ale Bruksela. W skrócie: to nie jakiś biurokrata w Warszawie unieważniałby niegrzecznym obywatelom ubezpieczenia, ale unijny eurokrata. Nawet w zaprowadzaniu reżimu i pozbawianiu wolności nie byłibyśmy suwerenni, tylko zdani na Brukselę.

Oczywiście Komisja nie planuje poprzestać na eID. Kolejną rzeczą, nad którą pracują władcy Europy jest cyfrowe euro. Komisarz Unii ds rynku wewnętrznego i usług Thierry Breton, ten sam, który zaprowadza cenzurę w mediach społecznościowych oznajmił: *Teraz, gdy mamy portfel tożsamości cyfrowej, musimy coś do niego włożyć.*

Oczywiście chodzi też o pieniądze. W unijnym portfelu mają znaleźć się nie tylko cyfrowe dokumenty, ale też cyfrowe

pieniądze. To znakomicie ułatwia kontrolę i zaprowadzanie systemu kredytu społecznego. I znów – jak w Kanadzie, czy Brazylii, protestujący obywatele mogą zostać jednym kliknięciem” pozbawieni dostępu do swych kont, a więc pieniędzy. Nie wypłacą ich, nie dokonają nawet najbardziej podstawowej transakcji, bo ich karty i urządzenia elektroniczne będące nośnikami cyfrowej waluty przestaną działać.

Catherine Austin Fitts amerykańska ekspertka finansowa i była sekretarz mieszkalnictwa w rządzie George’a Busha ostrzega, że cyfrowy system będzie kontrolowany centralnie, a środki finansowe każdej osoby mogą być ograniczane.

*Możliwość dokonywania transakcji finansowych można wyłączyć. Powiedzmy, że chcę zmusić cię do przyjęcia szczepionki. Jeśli nie zrobisz tego, co ci każę, będzie można odmówić ci dostępu do środków finansowych, albo całkowicie je zablokować.*

Taki system totalitarny mógłby również pozwolić państwu kontrolować też na co obywatele wydają swoje pieniądze. O tym, że nie jest to imaginacja, abstrakcja świadczy właśnie zablokowanie pieniędzy obywatelom w Kanadzie, czy protestującym przeciwko prezydentowi Luli w Brazylii.

Teoretycznie pieniądź cyfrowy ma być dużym ułatwieniem, ale jest znakomitą narzędziem kontroli pozbawiającym nas też prawa do prywatności.

*Fintech i CBDC (pieniądz cyfrowy) niosą ze sobą konsekwencje społeczne. Gdyby gotówka ustąpiła miejsca CBDC, a systemy płatności były cyfrowe, wszelkie pojęcie anonimowości i prywatności w sprawach finansowych byłoby poważnie zagrożone.*

pisze amerykański ekonomista, profesor Cornell University Eswara Pasada w swej książce „Przyszłość pieniądza. Jak

rewolucja cyfrowa przemienia świat walut i finansów”.

*CBDC stałoby się też narzędziem umożliwiającym wdrażanie różnych rządowych polityk gospodarczych i społecznych.*

Przed niebezpieczeństwem waluty cyfrowej ostrzega też Adam Glapiński.

*Nie można wykluczyć, że są wydatki...o których konsument nie chciałby informować swojego banku. W tym kontekście należałoby rozważać proponowaną regulację również w odniesieniu do prawa do prywatności konsumentów wobec przedsiębiorców, tym bardziej że ochrona tej prywatności została expressis verbis wyrażona m.in. w art. 76 Konstytucji RP*

– pisze prezes w liście do resortu finansów, który jest gorliwym zwolennikiem likwidacji gotówki, prezes NBP.

Edward Dowd, założyciel Phinance Technologies ostrzega, że każdy system CBDC będzie systemem totalitarnej kontroli powiązanej z „kredytem społecznym” w stylu chińskim. Nieposłuszni obywatele będą odcinani od pieniędzy, ale też dostępu do usług publicznych.

*Pieniądz cyfrowy Staje się po prostu narzędziem inżynierii społecznej, gadżetem maniaka kontroli.*

mówi Dowd.

Wszystko się ze sobą wiąże. To system, a nie pojedyncze, rozproszone działania. A więc trzeba pamiętać, iż forsowana w Brukseli zmiana Traktatów przewiduje likwidację walut krajowych i przymusowe zastąpienie ich euro. Polska nie tylko nie mogłaby prowadzić własnej polityki monetarnej, ale Unia kontrolowałaby też portfele, czyli pieniądze polskich obywateli.

Rządy przy pomocy cyfrowego pieniądza mogą nie tylko karać nieposłusznych obywateli, ale też kontrolować i dyscyplinować każdego, wymuszać określone zachowania w codziennej aktywności. Przykład płynie z uśmiechniętej, miłej i postępowej tyranii w Kanadzie. Spółdzielcza kasa oszczędnościową Vincyty wprowadziła karty, które zliczają ślad węglowy, jaki zostawiły kupowane z jej pomocą towary. Podobne rozwiązanie wprowadził australijski Commonwealth Bank. Mamy więc znów do czynienia z fikcją anonimowości. System precyzyjnie zbiera dane o tym, na co użytkownicy wydają swoje cyfrowe kochane pieniądze, przechowuje je i przetwarza. Teraz wystarczy wprowadzić limit śladu węglowego przypadającego na każdego obywatela. Po jego przekroczeniu nie będzie można dokonać transakcji

Nie należy mieć najmniejszych złudzeń co do złych intencji władców Europy. Wszystko zbiega się w czasie. Szefowa Europejskiego Banku Centralnego Christina Lagarde, właśnie oznajmiła o znacznych postępach banku w pracach nad walutą cyfrową. Tymczasem amerykańska Rezerwa Federalna praktycznie nie podjęła żadnych prac. Gotówka w Ameryce jest niezagrożona.

Europa obok Chin jest prymusem w konstruowaniu elektronicznych smyczy na obywateli. Do tego dzieła służy nawet nieszczęsne KPO. 20% pieniędzy z unijnych pożyczek, czy grantów, które będą spłacane nowymi podatkami musi być przeznaczone na tzw. transformację cyfrową.

Ale jest coś, co może sprawić, że na razie władcom Europy nie uda się zaprowadzić systemu permanentnej, wszechogarniającej kontroli elektronicznej. Tym czymś jest katastrofalny stan niemieckiej gospodarki cyfrowej. Niemcy są na przedostatnim miejscu w Unii jeśli chodzi o dostęp do szybkiego Internetu. Wszędzie brakuje infrastruktury, a wszystko wskazuje na to, że nie będą w stanie szybko zbudować sieci światłowodowej, która jest niezbędna do wydajnej transmisji danych. To kraj bez wykształconej kadry i anachronicznych urządzeń jak faks. Trudno myśleć o elektronicznym paszporcie tam gdzie nie

działają nawet najprostsze usługi online, czy o cyfrowym pieniądzu w kraju, w którym są kłopoty z płaceniem kartą.

Komisja Europejska ma 28 listopada głosować nad przyjęciem elektronicznego portfela Tymczasem nie wiemy nawet jakie stanowisko reprezentuje obecny polski rząd. Jak nasz przedstawiciel głosował na Radzie Unii Europejskiej. O tym jaką postawę zajmie przyszły rząd możemy myśleć z prawdziwą trwogą. Nie ma wątpliwości, że eurokraci chcą domknąć system i zbudować uśmiechnięty liberalny reżim, w którym obywatele są sprowadzeni do roli konsumentów, a wszystko kontrolują władcy i właściciele Europy.

[Dariusz Matuszczak](#)

---

**Aplikacje należące do Facebooka mogą śledzić i zbierać Twoje dane, nawet jeśli nie używasz ich aktywnie**



Wiele aplikacji na smartfony [śledzi dane osób](#), w tym ich bieżącą lokalizację, nawet jeśli nie korzystają z nich aktywnie. Eksperci twierdzą, że jednym z najgorszych

przestępców jest Facebook Messenger, dedykowana aplikacja do przesyłania wiadomości firmy mediów społecznościowych.

Eksperci zachęcają teraz ludzi do przeprowadzenia badań i zastanowienia się, jakie dane osobowe mogą rozdawać, pobierając i rejestrując się w aplikacjach takich jak Facebook Messenger.

„Jestem świadomy tego, kogo zaprosić do mojego domu, więc myślałem tak samo o tym, co mam na telefonie, i zachowałem ostrożność przy pobieranych aplikacjach” – powiedział Michael Huth, dyrektor ds. Badań i współzałożyciel firmy zajmującej się prywatnością i zorientowaną przeglądarką z własną wyszukiwarką i aplikacją.

Huth poradził ludziom, aby obniżyli poziom tego, do czego Facebook Messenger może uzyskać dostęp ze swoich smartfonów. [Aplikacja Facebook](#) może zbierać wszelkiego rodzaju dane od swoich użytkowników, jeśli tego nie robią, zwłaszcza jeśli nie są świadomi, do czego aplikacja ma dostęp.

„Firmy takie jak Google i Facebook próbują ukryć to, co robią z danymi i sprawić, by brzmiały pozytywnie”, powiedział współzałożyciel i dyrektor generalny Xayn Leif-Nissen Lundbaek. „Zawierają język, który brzmi tak, jakby chroniły prywatność, chociaż tak nie jest”.

Innym przykładem, który podał Lundbaek, jest WhatsApp, rzekomo prywatna usługa przesyłania wiadomości należąca do Facebooka z szyfrowaniem typu end-to-end.

Lundbaek powiedział, że WhatsApp oferuje niewiele funkcji, które według Facebooka poprawiają jego prywatność. W rzeczywistości te funkcje w niewielkim stopniu chronią dane osób.

„Istnieje szereg aplikacji, takich jak przeglądarka Google i TiKTok, które są gorsze niż WhatsApp, ale nadal nie jest to dobry przykład” – powiedział. „To nie jest obrońca

prywatności”.

„Śledzą wszystko, od interakcji po inne używane aplikacje, lokalizacje i ruch” – dodał Lundbaek.

## **Inne aplikacje należące do Facebooka przekazujące dane użytkownika firmie macierzystej**

Facebook Messenger, WhatsApp i Instagram są własnością Facebooka. Wszystkie są znane [z udostępniania wielu prywatnych danych](#) firmie macierzystej.

Obecne zasady WhatsApp chronią zawartość czatów danej osoby, w tym zdjęcia, filmy i połączenia, przed przechwyceniem przez Facebook. Nie wiadomo, czy niniejsza polityka prywatności jest przestrzegana co do joty.

To, co usługa szyfrowanych wiadomości typu end-to-end może udostępniać, to numer telefonu i nazwa profilu użytkownika. Może również udostępniać, gdy użytkownik wysyła wiadomość do innych osób. Adres IP użytkownika może być również gromadzony i udostępniany innym markom należącym do Facebooka.

Polityka prywatności WhatsApp jest celowo niejasna. Mówi, że może udostępniać dane osobowe Facebookowi wyraźnie wyróżnione w polityce „lub uzyskane po powiadomieniu lub na podstawie Twojej zgody”.

Niedawna zmiana w polityce prywatności WhatsApp umożliwiła również firmom reklamującym się za pośrednictwem Facebooka przechowywanie czatów użytkowników na serwerach należących do Facebooka. Zak Doffman, dyrektor generalny firmy Digital Barriers zajmującej się technologią monitoringu, powiedział, że podważa to wiarygodność WhatsApp jako rzekomo kompleksowej usługi szyfrowanej wiadomości.

„WhatsApp twierdzi, że Facebook nie może wykorzystywać tych danych, ale firma może wyszukiwać czaty w celach reklamowych” – powiedział Doffman.

Instagram jest o wiele bardziej bezpośredni dzięki zbieranym danym. Jego polityka prywatności stwierdza, że „Facebook „łączy informacje o twoich działaniach w różnych produktach i urządzeniach Facebooka”. Aplikacja podobno robi to, aby zapewnić użytkownikom „bardziej dostosowane i spójne wrażenia”.

Ponadto Instagram swobodnie gromadzi lokalizacje użytkowników, miejsca zamieszkania, miejsca, które odwiedzają, oraz szczegóły dotyczące firm i osób, z którymi są blisko i z którymi wchodzi w interakcje, aby „dostarczać, personalizować i ulepszać produkty Facebooka”.

Innymi słowy, Instagram udostępnia te dane Facebookowi w celu reklamy ukierunkowanej.

Jake Moore, specjalista ds. cyberbezpieczeństwa, ostrzegł osoby, które chcą korzystać z Instagrama, że „ma on mniej kontroli prywatności niż sam Facebook.

„Instagram ma mniej kontroli prywatności niż Facebook” – powiedział. „I nie można powstrzymać większości swoich danych między platformami”.

**Źródło:**

[The-Sun.com](https://www.the-sun.com)

[Wired.co.uk](https://www.wired.co.uk)

---

# Chiny chcą kontrolować globalny system „paszportów szczepionkowych”



Komunistyczne Chiny [zwracają się do Światowej Organizacji Zdrowia \(WHO\)](#) o pozwolenie na zbudowanie globalnego systemu nadzoru „paszportu szczepionkowego”, który według autorytarnego reżimu mógłby zostać uruchomiony w ciągu tygodnia, gdyby dostali zielone światło.

Komunistyczna Partia Chin już ustanowiła w Chinach system paszportów szczepionkowych, który jest [bezpośrednio powiązany z ich systemem zaufania społecznego](#).

Mieszkańcy Chin, którzy zostali zaszczepieni na koronawirusa z Wuhan (Covid-19), mogą podróżować i prowadzić interesy „normalnie”, podczas gdy ci, którzy nie zostali zaszczepieni, nie mogą wykonywać takich czynności, dopóki nie zgodzą się na zastrzyk.

„Oceny” przyznawane są mieszkańcom Chin na podstawie ich współpracy z agendą reżimu. Jeśli KPCh pochwała twoje zachowanie, otrzymujesz wyższy „wynik”. Jeśli powiesz złe rzeczy o reżimie, Twój wynik się zmniejszy.

Celem Chin jest rozszerzenie tego systemu zarządzania i kontroli na całym świecie. Osoby, które zostaną zaszczepione przeciwko chińskiemu wirusowi, otrzymają „stempel” w paszporcie szczepionkowym, umożliwiający im wejście na pokład pociągów i samolotów, a ci, którzy odrzucają szczepionkę,

otrzymają polecenie pozostania w domu.

WHO wyraźnie poinstruowała kraje członkowskie, aby nie konstruowały takiego systemu, ponieważ dostępność szczepionek nie jest jeszcze „sprawiedliwa”. Jednak komunistyczne Chiny przeciwstawiają się WHO i naciskają na globalne przyjęcie swojego systemu paszportów szczepionkowych.

„Chińscy eksperci zauważyli we wtorek, że Chiny mogą pomóc, dzieląc się swoimi doświadczeniami z WHO i zapewniając wsparcie techniczne w organizacji problemu”, donosi *Global Times*, gazeta propagandowa prowadzona przez KPCh w Chinach.

„... Chiny są najbardziej doświadczonym krajem na świecie w stosowaniu systemu kodów zdrowotnych, podczas gdy WHO jest najwłaściwszym organizatorem tej sprawy, aby zapewnić niezależność, uczciwość i bezpieczeństwo danych” – dodał.

## **Komunistyczne Chiny chcą rządzić światem**

Chiny od dawna obserwują, śledzą i naruszają prawa człowieka swoich obywateli, którzy nie mają prawie żadnej swobody poruszania się bez „pozwolenia” ich zwierzchników. Reżim nie chciałby niczego więcej, jak tylko rozszerzyć ten system przymusowej niewoli na wszystkie inne narody na ziemi.

„Jeśli chodzi o technologię, uważam, że chińskie firmy mogą zbudować międzynarodową platformę w zaledwie tydzień” – powiedział komunistyczny chiński „ekspert”, cytowany w artykule *Global Times* o tym, jak łatwo byłoby zglobalizować system.

„WHO może opracować zasady, procedury i format danych”, mówi dalej ten ekspert, który kieruje grupą zwaną „Information Consumption Alliance”. „Chiny są bardzo chętne do udzielenia wsparcia w zakresie wymiany doświadczeń i technik tworzenia takiej platformy, ponieważ kraj ten ma w tym bogate doświadczenie”.

The *Global Times* twierdzi, że globalny system nadzoru zarządzany przez komunistyczne Chiny w jakiś sposób „gwarantowałby zaufanie publiczne”. W międzyczasie WHO, które jest zaniepokojone tym, co może nadejść dalej, skapitulowało przed większością innych żądań Chin podczas tej „pandemii”.

Stany Zjednoczone już teraz mają przedsmak tego komunistycznego spisku [w mediach społecznościowych](#), gdzie na przykład użytkownicy Facebooka są obecnie szeroko śledzeni i ankietowani oraz otrzymują „oceny” na podstawie ich zachowania w Internecie.

Komunistyczne Chiny naciskają również na Joe Bidena, znanego jako „China Joe”, by uznał reżimową „domową” szczepionkę za „bezpieczną i skuteczną” opcję zgodności z proponowanym globalnym programem paszportów szczepionkowych.

„Chińscy eksperci stwierdzili, że jest bardzo możliwe i praktyczne, aby Chiny rozpoczęły wzajemne uznawanie z krajami, które zatwierdziły chińskie szczepionki, takimi jak Malezja, Singapur i Indonezja”, donosi *Global Times*.

**Źródła:**

[Breitbart.com](#)

[NaturalNews.com](#)

Artykuł przetłumaczono z [newstarget.com](#)

---

# Nowozelandzkie

# „0bozy”

# 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](https://www.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](https://humansarefree.com)

---

# Pekin wykorzystuje pandemię koronawirusa do rozbudowy aparatu nadzoru internetowego



Według raportu Freedom House, Pekin wykorzystuje pandemię koronawirusa w Wuhan (COVID-19) jako uzasadnienie rozszerzenia i zintensyfikowania i tak już gigantycznych [systemów nadzoru internetowego](#).

W swoim corocznym raporcie Freedom of the Net, w którym [szczegółowo opisano stan nadzoru cyfrowego](#) w ponad 60 krajach, organizacja non-profit umieściła Chiny na ostatnim miejscu z wynikiem [10 na 100](#). To szósty rok z rzędu, w którym kraj ten został ukoronowany jako „najgorszy gwałciciel wolności w internecie” na świecie.

*„Ta pandemia normalizuje rodzaj cyfrowego autorytaryzmu, który Komunistyczna Partia Chin (KPCh) od dawna stara się wprowadzić do głównego nurtu” – napisał Freedom House w oświadczeniu.*

Według raportu, chińskie władze wdrożyły zarówno niską, jak i zaawansowaną technologię, aby kontrolować swobodny przepływ informacji w Internecie na temat stanu tzw. pandemii koronawirusa w tym kraju. Wykorzystały również te technologie, aby uniemożliwić użytkownikom Internetu przeglądanie niezależnych źródeł wiadomości, które kwestionują oficjalną narrację KPCh.

Freedom House zauważył również, że na początku tzw. pandemii Chiny próbowały bagatelizować i ignorować ostrzeżenia lekarzy dotyczące pierwotnego wybuchu koronawirusa w Wuhan. Odkryli również, że mniej użytkowników internetu w Chinach z powodzeniem omija krajową Wielką Zaporę Sieciową, zwłaszcza po zaostrzeniu przez Pekin ograniczeń dotyczących osób korzystających z wirtualnych sieci prywatnych w celu uzyskania dostępu do zablokowanych witryn.

W raporcie stwierdza się ponadto, że tylko w pierwszym kwartale 2020 r. Chińska Administracja Cyberprzestrzeni, główny regulator internetowy w kraju, zamknęła 816 stron internetowych i usunęła ponad 33000 kont i grup na zatwierdzonych witrynach społecznościowych, takich jak Renren, Weibo i WeChat.

Masowa ekspansja wysiłków w zakresie inwigilacji Internetu w tym kraju spowodowała również wzrost liczby „fabryk cenzury”. W tych miejscach pracy znajdują się tysiące cenzorów internetowych, którzy zamiatają przestrzeń internetową kraju za pomocą technologii sztucznej inteligencji.

Chiny nie są jedynym krajem wykorzystującym COVID-19 do uzasadnienia ekspansji możliwości [nadzoru internetowego](#). Zarówno podmioty państwowe, jak i niepaństwowe wdrażają nowe technologie, które w dowolnym momencie przed globalną pandemią byłyby uważane za zbyt inwazyjne.

Pozostałe kraje, które [dołączają do Chin w pierwszej piątce](#), to Iran, Syria, Kuba i Wietnam. Pięć najlepszych krajów to Islandia, Estonia, Kanada, Niemcy i Wielka Brytania. Tajwan nie został uwzględniony w rankingu pomimo tego, że był znany jako [drugi najbardziej wolny kraj w Azji](#).

## **Technologia nadzoru przeciw dysydentom jest wdrażana jako instrumenty „zdrowia publicznego”**

Sarah Cook, starszy badacz w Freedom House, twierdzi, że wiele nowych chińskich technologii inwigilacji zostało po raz

pierwszy opracowanych w celu ochrony kraju przed dysydentami. W szczególności Cook zauważa, że 5G-technologia opracowana przeciwko Ujgurom i innym mniejszościom muzułmańskim w Xinjiangu rośnie obecnie w innych częściach kraju.

Jedną z takich technologii przeciwdziałania dysydemom jest urządzenie przenośne, którego władze mogą używać do skanowania smartfonów ludzi i pobierania z nich danych bez zgody właściciela.

*„Rząd Chin już teraz korzysta z najbardziej wyrafinowanego i wielowarstwowego aparatu cenzurującego i kontrolującego Internet na całym świecie” – powiedziała Cook.*

Istniejąca technologia nadzoru przeciwko dysydemom jest również udoskonalana na potrzeby epoki pandemii. W marcu, kiedy koronawirus dopiero zaczynał rozprzestrzeniać się po całym świecie, Chiny były już bliskie ulepszenia swojej technologii rozpoznawania twarzy [w celu identyfikacji osób noszących maski](#).

Inne technologie, zarówno stare, jak i nowe, są również wykorzystywane do naruszania prywatności obywateli Chin, na przykład zmuszając ludzi do korzystania z aplikacji, która śledzi infekcje i zmuszając ludzi do umieszczania kamer internetowych w ich domach i poza ich drzwiami, aby śledzić ich ruchy. Cook twierdzi, że te systemy mają tylne drzwi, które pozwalają policji nadzorować ludzi, kiedy tylko zechcą.

Według Cooka rozprzestrzenianie się pandemii jest bezpośrednio związane z ekspansją kontroli KPCh nad mową w Internecie.

Warto zadać sobie pytanie: jak się ma sytuacja w Polsce, jeżeli chodzi o aplikacje nadzorujące osoby objęte kwarantanną...?

**Źródła:**

[TheEpochTimes.com](http://TheEpochTimes.com)

[VOANews.com](http://VOANews.com)

[TaiwanNews.com.tw\\_1](http://TaiwanNews.com.tw_1)

[FreedomHouse.org](http://FreedomHouse.org)

[TaiwanNews.com.tw\\_2](http://TaiwanNews.com.tw_2)

[FT.com](http://FT.com)

---

# Kalifornia zakazuje stosowania technologii rozpoznawania twarzy w nagraniach z kamer policjantów



Kalifornia może mieć wiele wątpliwych praw, ale jest takie, które zasługuje na aplauz. Zabrania stosowania technologii rozpoznawania twarzy w [nagraniach wykonanych przez kamery funkcjonariuszy policji](#).

Rozpoznawanie twarzy to technologia, która polega na dopasowywaniu w czasie rzeczywistym obrazu osoby do jej

poprzedniego zdjęcia. Opiera się na fakcie, że twarz każdej osoby ma około 80 unikalnych punktów węzłowych w obszarach nosa, ust, policzków i oczu, które można wykorzystać do odróżnienia ludzi od siebie.

Cyfrowa kamera wideo służy do pomiaru odległości między tymi punktami na twarzy osoby. Obejmuje między innymi pomiary głębokości oczodołów, odległości między oczami, kształtem linii żuchwy i szerokości nosa. Informacje te służą do tworzenia unikalnego kodu numerycznego, który można dopasować do kodu pobranego z poprzedniego zdjęcia.

W marcu Waszyngton stał się pierwszym stanem w kraju, który zalegalizował używanie rozpoznawania twarzy przez organy ścigania i inne agencje stanowe. Oprogramowanie było już używane na poziomie hrabstwa i miasta przed wprowadzeniem tam nowego prawa. Jednak rozpoznawanie twarzy może być używane tylko w niektórych przypadkach, takich jak poszukiwanie zaginionych osób lub identyfikacja zwłok. Agencje będą zobowiązane do złożenia zawiadomienia o zamiarze użycia systemu zanim go użyją, a także raportu dotyczącego odpowiedzialności.

Jeśli chodzi o ruch Waszyngtonu, American Civil Liberties Union stwierdziła, że "zamiast zabezpieczyć wykorzystanie rozpoznawania twarzy, grozi legitymizacją jego rozszerzenia. Kierownik projektu ACLU Jennifer Lee powiedziała, że "prawo zawiera język, który pozwala [agencjom na używanie rozpoznawania twarzy](#) do odmawiania ludziom podstawowych potrzeb i innych niezbędnych rzeczy, takich jak mieszkanie, jedzenie, woda i opieka zdrowotna.

## **Zwolennicy prywatności chwają ustawę CA.**

Zwolennicy prywatności [wyrazili ulgę](#), że ustawa kalifornijska została podpisana przez gubernatora Gavina Newsoma. Dotyczy to nie tylko rozpoznawania twarzy, ale także ogólnie nadzoru biometrycznego, takiego jak analiza chodu z wykorzystaniem

materiału filmowego, który można zebrać z materiału wideo z kamery policyjnej.

W projekcie ustawy stwierdza się: „Korzystanie z rozpoznawania twarzy i innego nadzoru biometrycznego jest funkcjonalnym odpowiednikiem wymagania od każdej osoby, aby zawsze okazywała dowód tożsamości ze zdjęciem, co stanowi naruszenie uznanych praw konstytucyjnych. Ta technologia umożliwia również śledzenie osób bez pozwolenia”.

Posunięcie to nastąpiło niedługo po tym, jak ACLU przeprowadziło badanie rozpoznawania twarzy, które wykazało, że program Amazon błędnie zidentyfikował ponad dwa tuziny kalifornijskich prawodawców jako przestępców.

Podobny zakaz został wprowadzony kilka miesięcy wcześniej przez San Francisco w związku z wykorzystywaniem przez rząd funkcji rozpoznawania twarzy do nadzoru, kilka innych amerykańskich miast zrobiło to samo.

Chiny mają przeciwny pogląd na technologię rozpoznawania twarzy, w pełni ją wykorzystując do śledzenia swoich obywateli. Służy również do tworzenia wyników społecznych, które dają tym, którzy są posłuszni KPCh, pewne korzyści w ich codziennym życiu i ograniczają ruch i wolności tych, których wyniki są niższe.

Niestety nowe prawo Kalifornii dotyczy tylko korzystania z tej technologii przez organy ścigania, a nie sektor prywatny. Niemniej jednak jest to krok we właściwym kierunku, o wiele więcej, niż możemy powiedzieć o wielu innych [prawach pochodzących z Kalifornii](#) .

**Źródła:**

[DailyMail.co.uk](https://www.dailymail.co.uk)

[Mashable.com](https://www.mashable.com)

[NaturalNews.com](https://www.naturalnews.com)