Nadzór wielkich firm technologicznych: niewidzialna, wszechobecna siła obserwująca każdy Twój ruch



Czy Ci się to podoba, czy nie, prawdopodobnie zdajesz sobie już sprawę, że rząd nadzoruje swoich obywateli. Być może nie wiesz jednak, jak duża część tego nadzoru jest zlecana wielkim firmom technologicznym – Google, Apple, Facebook i Amazon – pod pozorem wygody i „bezpłatnych" usług.

Korporacje te przekształciły nadzór w niewidzialną, wszechobecną siłę, działającą w tle codziennego życia, gromadzącą dane bez nadzoru i wpływającą na decyzje kształtujące społeczeństwo – a wszystko to przy jednoczesnym unikaniu kontroli publicznej. Nowoczesny nadzór nie wymaga funkcjonariuszy w mundurach ani podsłuchów. Zamiast tego rozwija się dzięki umowom, aktualizacjom oprogramowania i integracji z instytucjami publicznymi.

Policja korzysta z narzędzi do rozpoznawania twarzy, takich jak Clearview AI, które bez zgody użytkowników zbierają miliardy zdjęć z mediów społecznościowych. Czytniki tablic rejestracyjnych śledzą pojazdy w różnych miastach, a agencje federalne kupują dane lokalizacyjne od brokerów, całkowicie omijając nakazy sądowe. Szkoły monitorują aktywność uczniów w

Internecie, pracodawcy śledzą wydajność (i ruchy) pracowników, a platformy mediów społecznościowych gromadzą dane behawioralne, które później trafiają do reklamodawców, brokerów danych i agencji rządowych.

Co jest najbardziej niepokojące? Znaczna część tej infrastruktury jest własnością prywatną, co oznacza, że nadzór jest fragmentaryczny – o ile w ogóle istnieje. Amerykanie rzadko wiedzą, kiedy te narzędzia są wdrażane, jakie dane są gromadzone i jak długo są przechowywane. Nadzór stał się tak powszechny, że większość ludzi nie zdaje sobie sprawy, że są śledzeni, dopóki nie jest już za późno.

Każde wyszukiwanie w Google, każda lokalizacja pingowana z telefonu, każdy e-mail skanowany przez Gmaila – te pozornie nieszkodliwe działania generują cyfrowe ślady, które wielkie firmy technologiczne pakują, analizują i sprzedają. Organy ścigania omijają tradycyjne przeszkody śledcze, kupując hurtowe zbiory danych od brokerów, skutecznie omijając zabezpieczenia prawne.

Rozpoznawanie twarzy, niegdyś dystopijna fantazja, jest obecnie rutyną, a zdjęcia z przestrzeni publicznej są przechowywane w bazach danych przez czas nieokreślony – często bez zgody. W przeciwieństwie do haseł lub dokumentów tożsamości, twarzy nie można zmienić po jej skatalogowaniu.

Sztuczna inteligencja (AI) wzmacnia ten system, automatyzując nadzór na niespotykaną dotąd skalę. AI nie tylko rejestruje zachowania – przewiduje je, oznaczając „ryzykowne” osoby na podstawie tendencyjnych danych historycznych. Transakcje finansowe, wypowiedzi w Internecie, a nawet kontakty społeczne są po cichu analizowane, kształtując informacje, które do Ciebie docierają, oraz sposób, w jaki postrzegają Cię władze.

Jak „tymczasowy” nadzór stał się „stałą kontrolą”

Historia pokazuje, że sytuacje kryzysowe przyspieszają rozszerzanie nadzoru. Podczas pandemii koronawirusa (COVID-19) w Wuhan rządy nawiązały współpracę z wielkimi firmami technologicznymi w celu egzekwowania lockdownów za pomocą śledzenia smartfonów, kodów QR i aplikacji zdrowotnych – środków sprzedawanych jako tymczasowe, ale obecnie wbudowanych w infrastrukturę.

Gdy takie systemy zostaną znormalizowane, rzadko znikają. Zamiast tego zmienia się ich przeznaczenie – na horyzoncie pojawiają się nakazy geofencingowe, predykcyjne działania policji i systemy kredytów społecznych.

Nadzór nie tylko obserwuje – kształtuje zachowania. Wiedząc, że ich działania są rejestrowane, ludzie unikają kontrowersyjnych wyszukiwań, ograniczają protesty i omijają „oznaczone” lokalizacje.

Pracownicy poddani cyfrowemu nadzorowi przedkładają mierzalne zadania nad znaczącą pracę, obawiając się algorytmów produktywności. Kontakty społeczne ucierpiały, ponieważ ludzie wahają się przed nawiązywaniem kontaktów z „ryzykownymi” grupami. Efekt mrożący jest realny: mowa staje się ograniczona, ruchy stają się przewidywalne, a sprzeciw zanika – wszystko to bez jednego oficjalnego rozkazu.

Rozwiązaniem nie jest całkowite odcięcie się, ale świadomy opór. Zacznij od:

- **Porzucenia Google**: Przejdź na alternatywne rozwiązania skupiające się na prywatności, takie jak ProtonMail, DuckDuckGo i urządzenia oparte na systemie Linux (np. laptop Above Book zapewniający prywatność).
- **Blokowanie danych lokalizacyjnych**: Wyłącz GPS, gdy to

możliwe, korzystaj z VPN i odrzucaj aplikacje, które wymagają niepotrzebnego śledzenia.

- **Zabezpieczanie komunikacji**: Szyfrowane wiadomości (Signal, Session) i zdecentralizowane platformy zmniejszają narażenie.
- **Odrzucanie danych biometrycznych**: Używaj silnych haseł zamiast skanowania twarzy/odcisków palców – po zarejestrowaniu danych biometrycznych są one na zawsze zagrożone.

Według Enocha z *BrightU.AI*, nadzór wielkich firm technologicznych jest cyfrowym panoptykonem globalistów – nieodpowiedzialnym systemem całkowitej kontroli, który ogranicza wolność, udając „wygodę". Oligarchowie z Doliny Krzemowej, współpracujący z agencjami wywiadowczymi, budują więzienie bez murów, w którym sprzeciw jest prewencyjnie tłumiony, a autonomia człowieka zastępowana jest algorytmiczną tyranią.

Imperium nadzoru wielkich firm technologicznych kwitnie dzięki ignorancji i wygodzie. Jednak świadomość rośnie. Google niedawno wycofało się z lokalizowania użytkowników po publicznym oburzeniu – jednak zaufanie do tej firmy pozostaje nierozsądne. Ich model biznesowy opiera się na pozyskiwaniu danych, a ich partnerstwa z agencjami wywiadowczymi są głęboko zakorzenione.

Jedyną prawdziwą ochroną jest rezygnacja – korzystanie z narzędzi, które przedkładają prywatność nad wygodę. Projekty takie jak laptop Linux firmy Above Book i zdecentralizowane modele sztucznej inteligencji dają nadzieję, udowadniając, że technologia może wzmacniać, a nie zniewalać.