

„Przezroczysty obywatel” już dawno stał się rzeczywistością: sztuczna inteligencja odszyfrowuje „anonimowe” dane lokalizacyjne za 2,24 dolara

• 02 września 2026



(C) Raport 24/SI

Miliardy ludzi noszą smartfony praktycznie przez całą dobę, zostawiając za sobą ślad przez całe życie. Brokerzy danych od lat gromadzą i sprzedają takie informacje o lokalizacji jako rzekomo anonimowy towar. Szwajcarscy naukowcy wykazali teraz, jak niewiele jest w rzeczywistości „anonimowości”: średnio sztuczna inteligencja potrzebowała zaledwie 17 minut i 2,24 dolara, aby zidentyfikować konkretną osobę na podstawie danych o lokalizacji.

Smartfon wielokrotnie spędza noc pod tym samym adresem. Rano jedzie do biurowca, zostaje tam przez kilka godzin i wraca wieczorem. Nie trzeba być analitykiem wywiadu, żeby nabrać oczywistego podejrzenia: ktoś tu mieszka, ktoś tam pracuje. Oscar Thees, Roman Müller i Matthias Templ z Uniwersytetu Nauk Stosowanych w Północno-Zachodniej Szwajcarii zlecieli [to zadanie sztucznej inteligencji](#). Zaprojektowano ją tak, aby identyfikowała miejsca

zamieszkania i miejsca pracy na podstawie danych o ruchu, a następnie przeszukiwała publicznie dostępne informacje, aż do momentu, gdy za rzekomo anonimowym śladem GPS pojawi się nazwisko.

Wynik [powinien zainteresować każdego, kto nadal klika na strony internetowe z frazą „anonimizowane dane”](#). Spośród 25 osób badanych, których tożsamość można było zasadniczo ustalić na podstawie publicznie dostępnych informacji, system znalazł 18. Kiedy sztuczna inteligencja podawała konkretną nazwę, była ona poprawna w 18 na 19 przypadków. Przeciętny czas potrzebny na to wynosił zaledwie 17 minut i 2,24 dolara. Podczas gdy człowiek może przebadać ograniczoną liczbę osób jednocześnie, sytuacja wygląda zupełnie inaczej w przypadku wyszukiwań prowadzonych przez sztuczną inteligencję. Komputery mogą przetwarzać te zadania równolegle.

Anonimowość w zasadzie już nie istnieje.

Dane o lokalizacji są gromadzone, grupowane i sprzedawane masowo od lat. Brokerzy danych usuwają nazwy i inne oczywiste cechy identyfikacyjne, przypisując zamiast tego identyfikatory urządzeniom. Na papierze wygląda to na całkowicie anonimowe. W rzeczywistości wzorec ruchu często ujawnia więcej niż tylko nazwę w arkuszu kalkulacyjnym. Gdzie „śpi” urządzenie? Gdzie znajduje się między 20:00 a 17:00, od poniedziałku do piątku? Jaka firma się tam znajduje? Kto mieszka pod tym adresem i pracuje dla tej właśnie firmy? Nagle niewiele pozostaje z anonimowości.

Ze względu na ochronę prywatności danych, szwajcarscy naukowcy wykorzystali symulowane ślady GPS wokół rzeczywistych domów i miejsc pracy wolontariuszy. Ujawniło to, że poszukiwanie osoby, która kryje się za śladem danych o lokalizacji, można teraz z łatwością powierzyć sztucznej inteligencji. Takie rzekomo „anonimizowane” pakiety danych są łatwo dostępne.

Dane wykorzystywane do inwigilacji są od dawna sprzedawane.

Byłoby to o wiele mniej niepokojące, gdyby takie dane o lokalizacji były trudne do uzyskania. Ale jest dokładnie odwrotnie. „[Pliki brokerów danych](#)” ujawniły już skalę działalności branży. Dziennikarze z Netzpolitik.org i międzynarodowi partnerzy otrzymali ogromne pakiety danych od brokerów danych, czasami po prostu jako darmowe próbki dla potencjalnych nabywców. Jeden z badanych zbiorów danych zawierał około 380 milionów punktów danych o lokalizacji ze 137 krajów, powiązanych z około 47 milionami identyfikatorów urządzeń. Dane pochodziły z około 40 000 aplikacji, w tym takich jak Wetter Online, Focus Online, serwisy ogłoszeniowe i Flightradar24. W przypadku niektórych punktów danych smartfon można było zlokalizować z dokładnością do kilku metrów.

Zespół badawczy [twierdzi obecnie, że](#) posiada ponad 13 miliardów rekordów danych o lokalizacji od różnych dostawców. W Belgii dziennikarze znaleźli tysiące punktów danych o lokalizacji pochodzących z budynków UE i NATO. Około 2000 raportów o lokalizacji pochodziło z siedziby Komisji Europejskiej, około 5800 z Parlamentu Europejskiego i około 9600 z siedziby NATO. To wcale nie jest niewinna gra. Każdy, kto posiada takie dane, może poszukiwać pracowników rządowych, żołnierzy, dyplomatów lub funkcjonariuszy służb bezpieczeństwa. Z oficjalnych lokalizacji ślady przemieszczania się mogą potencjalnie prowadzić bezpośrednio do adresu prywatnego.

Błąd jest już w kieszeni spodni.

Report24 [donosił](#) już w styczniu o tym, jak dane reklamowe stały się prawdziwym narzędziem inwigilacji. Pod terminem „wywiad reklamowy” komercyjnie gromadzone informacje są analizowane w celu śledzenia urządzeń i tworzenia profili ruchu. To, co pierwotnie miało służyć bardziej ukierunkowanej reklamie, od dawna stało się przedmiotem zainteresowania organów bezpieczeństwa i służb wywiadowczych. Szwajcarskie badanie dodaje teraz kluczowy element do układanki. Nie wystarczy już polegać na fakcie, że w bazie danych przechowywany jest tylko identyfikator urządzenia, a nie jego nazwa. Sztuczna inteligencja może pomóc wypełnić właśnie tę lukę.

Po połączeniu urządzenia śledzącego z daną osobą, współrzędne stają się zapisem jej życia. Dom, miejsce pracy i regularne trasy to dopiero początek. Do tego dochodzą wizyty u lekarza, wydarzenia polityczne, demonstracje, kościoły, meczety, hotele, domy publiczne i inne miejsca, które nikogo nie obchodzą. Przestępcy mogą na podstawie tych danych wywnioskować wzorce absencji i nawyki. Zagraniczne agencje wywiadowcze mogą być zainteresowane pracownikami rządowymi i ich kontaktami. W przypadku reżimów autorytarnych dane te oferują możliwości prześladowania członków opozycji lub członków własnej diaspory, nawet za granicą. Infrastruktura do tego celu nie musi być budowana; ona już istnieje.

Sztuczna inteligencja przekształca górę danych w narzędzie do nadzoru.

Do tej pory istniał co najmniej jeden naturalny hamulec: ktoś musiał analizować dane. Miliony punktów lokalizacji to same w sobie gigantyczny stos współrzędnych. Dopiero analiza przekształca je w użyteczne informacje. A sztuczna inteligencja zaczyna teraz usuwać ten hamulec. Znajdzenie miejsca zamieszkania, identyfikacja pracodawcy, przeszukiwanie rejestrów publicznych, porównywanie możliwych nazwisk – takie zadania nagle nie wymagają już godzin ludzkich badań. W szwajcarskim eksperymencie system wykonał je za zaledwie kilka dolarów.

To przekształca komercyjne repozytorium danych w narzędzie, z którego mogą korzystać nawet mniejsze podmioty. Kompleksowa analiza nie wymaga już zasobów dużej agencji wywiadowczej. A każdy, kto korzysta z ogólnodostępnego modelu sztucznej inteligencji na swoim komputerze, nie potrzebuje nawet zgody komercyjnego dostawcy. Żadne warunki świadczenia usług przez korporację zajmującą się sztuczną inteligencją nie uniemożliwiają analizy, gdy model działa lokalnie.

Przezroczysty obywatel został już dawno stworzony.

Nadzór nad współczesnym człowiekiem nie zaczyna się od jakiejś superbazy danych rządowych. Sami generujemy niezbędne informacje każdego dnia. Smartfony śledzą naszą lokalizację. Różne aplikacje dostarczają dane sieciom reklamowym. Nowoczesne pojazdy gromadzą dane GPS i informacje o użytkowaniu. Kamery rejestrują tablice rejestracyjne, a płatności cyfrowe pozostawiają kolejne ślady. Każdy zestaw danych sam w sobie może wydawać się nieszkodliwy. Ale razem tworzą coraz bardziej szczegółowy obraz. Report24 [donosił](#) już o danych gromadzonych przez nowoczesne samochody i o tym, dlaczego agencje wywiadowcze również interesują się tymi informacjami.

Obietnica anonimowości była już krucha. Sztuczna inteligencja jasno pokazuje teraz, że najwyraźniej nikt nie jest już bezpieczny przed takimi środkami nadzoru. Branża reklamowa i jej brokerzy danych zgromadzili przez lata gigantyczną górę surowego materiału z naszych cyfrowych śladów. Teraz dostępne są narzędzia, które potrafią wyodrębnić z tych danych

nazwiska, adresy, miejsca pracy i profile przemieszczania się za bezcen. Przezroczysty obywatel nie pojawi się w przyszłości. On już tu jest. I ładuje swój własny mobilny lokalizator każdego wieczoru.