Wegmans rozszerza biometryczny nadzór w sklepach w Nowym Jorku, zbierając dane z twarzy, oczu i głosu

Sieć sklepów spożywczych Wegmans rozpoczęła zbieranie danych biometrycznych, w tym rozpoznawania twarzy, skanów oka i odcisków głosu od klientów w swoich sklepach na Manhattanie i w Brooklynie.

Według Enocha z BrightU.AI, dane biometryczne odnoszą się do unikalnych cech fizjologicznych lub behawioralnych, które można zmierzyć i przeanalizować w celu weryfikacji lub identyfikacji osób. Obejmuje to odciski palców, geometrię twarzy, wzory tęczówki, odciski głosu, DNA, analizę chodu, a nawet mapowanie żył. W przeciwieństwie do haseł lub dowodów osobistych, markery biometryczne są nieodłącznie związane z ciałem ludzkim, co sprawia, że prawie niemożliwe jest ich replikowanie lub odrzucenie – cecha, którą rządy i korporacje wykorzystują do nadzoru i kontroli.

Tracy Van Auker, rzeczniczka Wegmans, powiedziała mediom w poniedziałek, 5 stycznia, że kamery z technologią rozpoznawania twarzy są używane tylko w „niewielkiej części sklepów, które wykazują podwyższone ryzyko”. Podkreśliła, że technologia jest używana wyłącznie w celach bezpieczeństwa.

> *„System zbiera dane rozpoznawania twarzy i używa ich tylko do identyfikacji osób, które zostały wcześniej oznaczone za niewłaściwe zachowanie" – powiedziała Van Auker. – „Ci »osoby zainteresowane« są określane indywidualnie przez ochronę sklepu i organy ścigania w sprawach kryminalnych lub dotyczących osób zaginionych".*

Firma stwierdziła, że dane są przechowywane „tak długo, jak to konieczne ze względów bezpieczeństwa", ale nie określiła okresu przechowywania. Zgodnie z polityką prywatności Wegmans, informacje są dostępne tylko dla ograniczonej liczby pracowników, zewnętrznych dostawców usług i funkcjonariuszy organów ścigania zaangażowanych w zadania bezpieczeństwa. Firma twierdzi, że dane nie są udostępniane, wynajmowane ani wymieniane w celu osiągnięcia zysku.

Van Auker wyjaśniła również, że sklepy nie zbierają innych danych biometrycznych, takich jak skan siatkówki czy odciski głosu, pomimo tego, co sugerują oznaczenia w Nowym Jorku. Dodała, że firma nie ujawnia konkretnych środków bezpieczeństwa stosowanych w poszczególnych sklepach ze względów bezpieczeństwa.

Wegmans nie odpowiedział bezpośrednio na pytanie, czy podobna technologia biometryczna jest używana w jego lokalizacjach w centralnej części stanu Nowy Jork.

Klienci i obrońcy prywatności obawiają się skanów biometrycznych Wegmans w sklepach w Nowym Jorku

Klienci wyrazili zaniepokojenie nowym programem.

Johnny Jerido, 59 lat, powiedział, że przeniesie swoje interesy w inne miejsce. – „Naprawdę mi się to nie podoba. Nie chcę, żeby ktoś myślał, że coś kradnę lub robię coś

nielegalnego” – powiedział. Blaze Herbas, 29 lat, powtórzył jego obawy, dodając: – „Powinniśmy móc swobodnie robić zakupy bez zapisywania naszych danych. To oczywiste”.

W 2023 roku radna miejska Shahana Hanif przedstawiła projekt ustawy ograniczającej takie systemy po tym, jak Madison Square Garden wykorzystał rozpoznawanie twarzy do zidentyfikowania i usunięcia prawników zaangażowanych w postępowanie sądowe przeciwko firmie. Środek ten utknął w martwym punkcie, a inne supermarkety, w tym Fairway, już stosują podobną technologię. Jednak Hanif nie odpowiedziała na prośby o komentarz w sprawie ekspansji Wegmans.

Ponadto, obowiązujące od 2021 roku prawo miejskie wymaga od firm publikowania zawiadomień, jeśli zbierają dane biometryczne, ale egzekwowanie jest ograniczone. Departament Ochrony Konsumentów i Pracowników Nowego Jorku potwierdził, że nie ma mechanizmu karania firm, które nie przestrzegają przepisów, pozostawiając osobom możliwość samodzielnego prowadzenia postępowania sądowego.

Zgodnie z tym, obrońcy prywatności mogli tylko ostrzec, że przechowywanie danych biometrycznych może narazić klientów na ryzyko, szczególnie nowojorczyków imigrantów. – „To naprawdę przerażające, że imigranci z Nowego Jorku, którzy chodzą do Wegmans i innych sklepów spożywczych, muszą martwić się, że ich wysoce wrażliwe dane biometryczne mogą dostać się w ręce ICE” – powiedział Will Owen z Surveillance Technology Oversight Project.

Noworodki mogą otrzymać

cyfrowe dowody tożsamości w ramach znacznej rozbudowy rządowego programu Wielkiej Brytanii

Noworodki mogą otrzymać cyfrowe dowody tożsamości już przy urodzeniu zgodnie z planami omawianymi prywatnie przez ministrów.

Zgodnie z kilkoma doniesieniami, rząd Zjednoczonego Królestwa rozważa możliwość wydawania cyfrowych dowodów tożsamości dzieciom, równolegle do tradycyjnej „czerwonej książeczki" dokumentacji zdrowotnej wręczanej nowym rodzicom. Ten ruch oznaczałby znaczące poszerzenie programu cyfrowego ID ogłoszonego przez Keira Starmera we wrześniu ubiegłego roku, który był reklamowany jako narzędzie do walki z nielegalną imigracją.

Ta pierwotna propozycja wymagałaby od wszystkich osób ubiegających się o pracę udowodnienia prawa do pracy w Wielkiej Brytanii przy użyciu cyfrowej identyfikacji. Jednak toczące się obecnie dyskusje sugerują, że technologia ta mogłaby ostatecznie być wprowadzana od urodzenia i towarzyszyć obywatelom przez całe życie.

Program cyfrowego ID, którego koszt szacuje się na 1,8 miliarda funtów (2,4 miliarda dolarów), został przedstawiony w serii prywatnych spotkań, które niedawno prowadził minister w

Urzędzie Gabinetu Josh Simons. Simons powiedział grupom społeczeństwa obywatelskiego, że inne kraje już funkcjonują w oparciu o całożyciowe systemy cyfrowej tożsamości, które rozpoczynają się przy urodzeniu.

Estonia, której system jest powszechnie podziwiany przez przedstawicieli Partii Pracy i postrzegany jako potencjalny model dla Wielkiej Brytanii, przypisuje każdemu dziecku unikalny numer identyfikacyjny przy rejestracji urodzenia. Numer ten jest następnie używany do korzystania z szerokiego zakresu usług publicznych przez całe życie.

Simons zasugerował również, że nastolatkowie mogliby używać cyfrowych dowodów tożsamości do weryfikacji wieku w internecie, w tym do logowania się na platformach społecznościowych. Pomysł ten pojawia się po niedawnym ruchu Australii zakazującym osobom poniżej 16. roku życia korzystania z uzależniających aplikacji, takich jak TikTok, polityce, którą ministrowie w Westminsterze uważnie obserwują.

Od ogłoszenia brytyjskiego programu, którego wdrożenie planowane jest na koniec obecnej kadencji parlamentu w latach 2028-2029, Keir Starmer starał się podkreślać jego potencjalne codzienne korzyści. Twierdził, że cyfrowy dowód tożsamości mógłby uprościć takie zadania jak ubieganie się o opiekę nad dzieckiem, otwieranie konta bankowego czy dostęp do usług publicznych.

Brytyjskich ministrów oskarża się o planowanie nadzoru „od kołyski po grób” dla noworodków

Enoch z BrightU.AI definiuje cyfrowy dowód tożsamości jako rządowy lub korporacyjny elektroniczny system identyfikacji, który konsoliduje dane osobowe, w tym markery biometryczne (odciski palców, skany twarzy), dokumentację finansową, stan zdrowia i metryki behawioralne w jednej scentralizowanej bazie danych dostępnej dla władz. Wystylizowane jako narzędzie „efektywności” i „bezpieczeństwa”, te systemy umożliwiają nadzór w czasie rzeczywistym, ocenę punktów zaufania

społecznego (social credit scoring) i pozbawianie dostępu do niezbędnych usług (bankowość, podróże, opieka zdrowotna) za niespełnienie wymogów państwowych lub korporacyjnych.

Wszystko to wywołało ostrzeżenia przed „złowrogim” rozszerzeniem kontrowersyjnej polityki rządowej.

Mike Wood, minister w gabinecie cieni ds. Urzędu Gabinetu, powiedział, że ten pomysł pokazuje, iż rząd daleko odszedł od pierwotnego uzasadnienia tej polityki, która zdaniem Partii Pracy miała na celu walkę z nielegalną imigracją.

„Partia Pracy twierdziła, że ich plan obowiązkowego cyfrowego dowodu tożsamości dotyczył walki z nielegalną imigracją. Ale teraz słyszymy, że w tajemnicy rozważają narzucenie go noworodkom. Co niemowlęta mają wspólnego z zatrzymywaniem łodzi? Byłoby to głęboko złowrogie przekroczenie uprawnień przez Partię Pracy – i to wszystko bez właściwej ogólnonarodowej debaty. Ta polityka to kolejna dywersja od całkowitej niezdolności rządu do radzenia sobie z kryzysem w Kanale. Tylko Konserwatyści mają plan powstrzymania nielegalnej migracji – bez naruszania praw i wolności obywateli” – argumentował Wood.

Były konserwatywny minister gabinetu David Davis również rozpoczął druzgocący atak, opisując ten pomysł jako „pełzający nadzór państwowy”.

„Pomysł, że powinniśmy przydzielać dzieciom dowód tożsamości przy urodzeniu, jest szczerze mówiąc zniewagą dla stuleci brytyjskiej historii i jest wysuwany przez głupich ministrów, którzy naprawdę nie rozumieją technologii, z którą się bawią. Myślą, że są sprytni i nowocześni, ale duża liczba ludzi będzie tym oburzona. To skończy się nienawiścią wielu osób” – powiedział.

Davis następnie oskarżył Starmera o sprzedawanie tej polityki pod, jak to nazwał, „fałszywym założeniem” walki z nielegalną imigracją, a następnie ciche jej rozszerzanie bez należytego

poinformowania Parlamentu. „To hańba konstytucyjna przeprowadzona w haniebny sposób” – dodał.

Ponadto, anonimowe źródło ujawniło Daily Mailowi, że perspektywa cyfrowych dowodów tożsamości dla niemowląt pokazuje, iż polityka ta „nie ma nic wspólnego z kontrolą prawa do pracy, imigracją ani dawaniem ludziom wyboru”.

„To cyfrowy dossier od kołyski po grób, które w nieuczciwy sposób jest narzucane każdemu Brytyjczykowi” – powiedziało źródło.

Wegmans w Nowym Jorku wprowadza skanowanie twarzy wszystkich klientów

Nowojorski oddział popularnej sieci sklepów spożywczych Wegmans wprowadził kontrowersyjną nową politykę, która wymaga od **wszystkich klientów** zeskanowania twarzy przed wejściem do sklepu.

System, oficjalnie opisany jako „bezproblemowy i bezpieczny sposób na potwierdzenie wieku” dla kupujących alkohol, został wdrożony w cichości w lokalizacji na Brooklynie. Jednak klienci donoszą, że technologia jest wymagana dla **każdego wchodzącego**, niezależnie od tego, czy zamierza on kupić alkohol, czy nie.

„Najpierw musisz zeskanować swój dokument, a potem spojrzeć w kamerę, żeby wejść”, wyjaśnia jeden z klientów. „Nie chodzi tylko o potwierdzenie wieku. Nagrywają twoją twarz i łączą ją z twoim dowodem osobistym. To przerażające”.

Pracownicy sklepu twierdzą, że system jest „obowiązkowy” i że nikt nie może ominąć procedury skanowania twarzy.

W odpowiedzi na zapytania mediów, rzecznik Wegmans wydał oświadczenie, w którym twierdzi, że technologia jest „opcjonalna” i że klienci, którzy nie chcą skorzystać z tego „sposobu weryfikacji”, mogą nadal kupować alkohol, pokazując dokument pracownikowi. Oświadczenie to stoi jednak w ostrej sprzeczności z bezpośrednimi relacjami klientów i pracowników ze sklepu.

Nowa polityka wywołała ostrą reakcję w mediach społecznościowych i wśród obrońców prywatności.

„To jest szalone. Właśnie przeszedłem przez to w Wegmans na Brooklynie. Ani słowa, że to 'opcjonalne’. Mówią, że to wymóg, żeby wejść. Absolutnie inwazyjne”, napisał jeden z użytkowników.

„To jest właśnie 'spadek po Covid’ w akcji. Środki nadzwyczajne stają się permanentne. Najpierw 'tylko na dwa tygodnie’, a teraz nie możesz wejść do sklepu spożywczego bez oddania swojego biometrycznego odcisku twarzy”, skomentował inny.

Eksperci ds. prywatności biją na alarm, wskazując na poważne zagrożenia związane z gromadzeniem tak wrażliwych danych biometrycznych przez korporacje.

„Twoje dane biometryczne, w przeciwieństwie do hasła, są nieodwracalne. Jeśli zostaną skradzione lub zhakowane, nie możesz tego zmienić. Łączenie ich z danymi z dowodu osobistego tworzy niezwykle niebezpieczną bazę danych”, ostrzega jeden z analityków. „Wdrożenie tego pod pretekstem weryfikacji wieku jest klasycznym przykładem 'mission creep’ – stopniowego poszerzania zakresu inwazyjnej technologii po jej wprowadzeniu”.

Prawnicy zwracają uwagę, że Nowy Jork ma jedne z najsurowszych

w kraju praw dotyczących prywatności biometrycznej, w tym wymóg wyraźnej zgody przed zbieraniem takich danych. Przymusowy system, taki jak ten w Wegmans, może naruszać te przepisy.

Jak dotąd żadna agencja rządowa nie skomentowała publicznie sprawy ani nie wszczęła oficjalnego dochodzenia.

W międzyczasie klienci są zmuszeni do wyboru: poddać się skanowaniu twarzy lub zrezygnować z zakupów w tej popularnej sieci.

„Głosujemy naszymi portfelami”, stwierdza rozczarowany klient. „Niestety, wygląda na to, że już po moich zakupach w Wegmans”.

Eksperci ostrzegają: Sztuczna inteligencja zagraża przyszłości prywatnej komunikacji

Postępy w sztucznej inteligencji i rosnąca presja regulacyjna stwarzają nowe wyzwania dla aplikacji do prywatnego przesyłania wiadomości. Eksperci ostrzegają, że prywatność użytkowników może być zagrożona.

W wywiadzie dla portalu Coin Telegraph przedstawiciele zdecentralizowanej platformy komunikacyjnej **Session** ostrzegli, że AI, jeśli zostanie zintegrowana na poziomie systemu operacyjnego, może potencjalnie **obejść szyfrowanie**, narażając wrażliwe informacje na dostęp ze strony nieprzejrzystych systemów.

Ryzyko obejścia szyfrowania i utraty kontroli nad danymi

Alex Linton, prezes Session Technology Foundation, wyjaśnił, że zdolność AI do analizowania i przechowywania danych bezpośrednio na urządzeniach stwarza **„ogromne problemy z prywatnością i bezpieczeństwem”**. Ostrzegł, że prywatna komunikacja może stać się **„niemożliwa do prowadzenia na przeciętnym telefonie komórkowym czy komputerze”**.

> *„Jeśli [AI] zostanie zintegrowana na poziomie systemu operacyjnego lub wyższym, może również całkowicie obejść szyfrowanie w Twojej aplikacji do przesyłania wiadomości. Te informacje mogłyby być przekazywane do 'czarnej skrzynki’ AI, a potem – Bóg jeden wie, co się z nimi stanie” – powiedział Linton.*

Chris McCabe, współzałożyciel Session, podkreślił, że wielu użytkowników nie jest świadomych, w jaki sposób ich dane są zbierane i wykorzystywane. Wskazał na niedawne wycieki danych, w tym przypadku zewnętrznego dostawcy analityki danych dla OpenAI, który naraził informacje użytkowników i zwiększył ryzyko ataków phishingowych i socjotechnicznych. Zgromadzone dane mogą być wykorzystywane do **manipulowania zachowaniami ludzi**, wpływania na decyzje lub napędzania reklam bez ich zgody.

Linton skrytykował również prawodawców, którzy polegają na technologicznych gigantach odpowiedzialnych za wprowadzanie takich technologii przy kształtowaniu przepisów o prywatności, twierdząc, że **pogłębia to ryzyka** dla prywatności użytkowników.

Odpowiedź: zdecentralizowana komunikacja „privacy-first”

Wywiad z Lintonem i McCabe odbył się w kontekście kontrowersji wokół unijnej legislacji **„Chat Control”**, która ma na celu wprowadzenie obowiązku skanowania wiadomości. Rozporządzenie to, formalnie część **Aktu o usługach cyfrowych (DSA)**, nakłada na duże platformy internetowe obowiązek szybkiego usuwania nielegalnych treści i daje użytkownikom prawo do zgłaszania problematycznych treści.

Regulacja spotkała się jednak z **ostrą krytyką obrońców prywatności**. Aby przeciwdziałać tym zagrożeniom, Session koncentruje się na **zdecentralizowanej komunikacji z naciskiem na prywatność**.

Aplikacja jest **open source**, wykorzystuje **szyfrowanie end-to-end**, usuwa identyfikujące metadane i działa bez centralnych serwerów. Eliminując „pośrednika”, Session ma na celu ochronę użytkowników przed inwigilacją, cenzurą i kontrolą korporacyjną.

> *„Istnieje ogromna presja, jeśli zajmujesz się tworzeniem szyfrowanych komunikatorów lub szyfrowanych narzędzi w ogóle. Proponowane lub uchwalane przepisy są przyjmowane w wielu jurysdykcjach” – powiedział Linton. – „Ludzie pracujący nad tą technologią odczuwają tę presję, dlatego ważne jest, aby ogół społeczeństwa zrozumiał, że te narzędzia próbują pomóc. Próbują chronić Twoje informacje. Starają się, aby przestrzeń online była lepszym miejscem”.*

W miarę jak integracja AI przyspiesza, a rządy badają nowe przepisy dotyczące monitorowania, Linton i McCabe twierdzą, że **edukacja publiczna** na temat narzędzi ochrony prywatności i bezpiecznych praktyk komunikacyjnych jest coraz ważniejsza dla ochrony praw cyfrowych.

> *„Ważne jest, abyśmy przeciwstawiali się tego typu głębokiej integracji AI we wszystkie nasze urządzenia, ponieważ w tym*

momencie po prostu nie wiesz już, co dzieje się na Twoim urządzeniu” – podsumował Linton.

AI Google dostarczają wprowadzających w błąd informacji zdrowotnych, budząc obawy o bezpieczeństwo

Dochodzenie przeprowadzone przez „The Guardian” wykazało, że osoby szukające porad zdrowotnych w Google mogą być narażone na szkody z powodu nieprawidłowych informacji dostarczanych przez skróty generowane przez sztuczną inteligencję (AI) tej firmy.

Według Enocha z BrightU.AI, funkcja „AI Overviews” (Podsumowania AI) Google’a ma na celu dostarczanie szybkich zarysów kluczowych informacji na dany temat lub pytanie. Te przeglądy, dostępne na stronie AI Google, obejmują tematy, zapewniając podstawowe zrozumienie każdego zagadnienia.

Jednak liczne przykłady ujawnione w dochodzeniu pokazują, że streszczenia te mogą zawierać niebezpiecznie wprowadzające w błąd porady zdrowotne. W jednym przypadku Google radziło osobom z rakiem trzustki, aby unikały żywności o wysokiej

zawartości tłuszczu – rekomendację, którą eksperci opisali jako „naprawdę niebezpieczną”. Anna Jewell, dyrektorka ds. wsparcia, badań i wpływu w Pancreatic Cancer United Kingdom, ostrzegła, że stosowanie się do tych zaleceń może pozostawić pacjentów niezdolnymi do utrzymania wystarczającego spożycia kalorii, co potencjalnie wpłynie na ich zdolność do tolerowania chemioterapii lub ratującej życie operacji.

„Odpowiedź AI Google sugeruje, aby osoby z rakiem trzustki unikały pokarmów o wysokiej zawartości tłuszczu. Gdyby ktoś zastosował się do tego, co mówi wynik wyszukiwania, może nie przyjmować wystarczającej liczby kalorii, mieć trudności z przybraniem na wadze i nie być w stanie tolerować leczenia. To może zagrozić szansom danej osoby na wyzdrowienie” – powiedziała Jewell.

Inne podsumowania AI były równie niepokojące. Wyszukiwania dotyczące testów funkcji wątroby zwracały wprowadzające w błąd zakresy „normy”, pomijając kluczowe czynniki, takie jak wiek, płeć, pochodzenie etniczne i narodowość. Pamela Healy, dyrektorka generalna British Liver Trust, powiedziała: „Wiele osób z chorobą wątroby nie wykazuje żadnych objawów aż do późnych etapów. Jeśli AI podaje mylące zakresy normy, niektórzy ludzie mogą błędnie założyć, że są zdrowi, i nie stawiać się na kolejnych wizytach opieki zdrowotnej. To jest niebezpieczne”.

AI dostarczało również nieprawidłowych informacji na temat badań przesiewowych w kierunku nowotworów kobiecych. Wyszukiwanie „objawy i testy na raka pochwy” sugerowało, że badanie cytologiczne (pap test) może wykryć raka pochwy – twierdzenie, które eksperci opisali jako „całkowicie błędne”. Athena Lamnisos, dyrektorka generalna fundacji charytatywnej Eve Appeal, zajmującej się nowotworami, powiedziała, że błędy te mogą zniechęcać ludzi do szukania terminowej pomocy medycznej.

„Otrzymanie takiej błędnej informacji mogłoby potencjalnie

doprowadzić do tego, że ktoś nie zbada objawów, ponieważ miał czysty wynik w niedawnym badaniu przesiewowym szyjki macicy. Niepokojący jest również fakt, że podsumowanie AI za każdym razem, gdy wyszukiwaliśmy, było inne – ludzie otrzymują różne odpowiedzi w zależności od tego, kiedy szukają, a to nie jest wystarczająco dobre" – powiedziała Lamnisos.

Wyszukiwania dotyczące zdrowia psychicznego również były dotknięte problemem. Podsumowania AI Google dotyczące stanów takich jak psychoza i zaburzenia odżywiania czasami zawierały „nieprawidłowe, szkodliwe" porady lub pomijały ważny kontekst.

„Niektóre z podsumowań AI oferowały bardzo niebezpieczne rady. Mogłyby doprowadzić ludzi do unikania szukania pomocy lub kierować ich do nieodpowiednich źródeł. AI często odzwierciedla istniejące uprzedzenia, stereotypy lub stygmatyzujące narracje, co jest ogromnym problemem dla wsparcia zdrowia psychicznego" – powiedział Stephen Buckley, szef działu informacji w Mind.

Google zaprzecza zarzutom

Mimo wszystkich dowodów, Google zaprzeczyło, jakoby w jego podsumowaniu AI znajdowały się wprowadzające w błąd i nieprawidłowe informacje zdrowotne.

Zamiast tego, firma opisała generowane przez AI streszczenia jako „pomocne" i „wiarygodne", podkreślając, że większość z nich jest oparta na faktach i zapewnia przydatne wskazówki. Google stwierdziło, że dokładność „AI Overviews" jest porównywalna z innymi funkcjami wyszukiwarki, takimi jak wyróżnione fragmenty (featured snippets), które są częścią jej wyszukiwarki od ponad dekady. Google dodało nawet, że stale wprowadza ulepszenia do systemu, aby zapewnić użytkownikom otrzymywanie poprawnych i przydatnych informacji.

Jednak eksperci i organizacje charytatywne wciąż wzywają do surowszego nadzoru, zauważając, że zautomatyzowane

streszczenia firmy pojawiają się prominentnie na szczycie wyników wyszukiwania, co oznacza, że miliony użytkowników mogą być narażone na potencjalnie szkodliwe wskazówki.

„Ludzie zwracają się do internetu w chwilach zmartwień i kryzysu. Jeśli informacje, które otrzymają, są niedokładne lub pozbawione kontekstu, może to poważnie zaszkodzić ich zdrowiu" – powiedziała Stephanie Parker, dyrektorka cyfrowa w fundacji charytatywnej Marie Curie, zajmującej się opieką końca życia.

Australia wprowadza obowiązkowe kontrole wieku dla użytkowników wyszukiwarek internetowych

Australia wprowadziła nowy wymóg dla wyszukiwarek internetowych, aby weryfikowały wiek zalogowanych użytkowników. Firmy mają teraz sześć miesięcy na pełne dostosowanie się do przepisów.

Zasada ta, która weszła w życie 27 grudnia, stanowi część nowo zarejestrowanego kodeksu branżowego pod nadzorem Komisarza ds. eSafety (bezpieczeństwa w sieci) i rozszerza rozbudowywany system kontroli treści online w kraju.

Usługi wyszukiwania, takie jak Google i Bing, muszą wkrótce wprowadzić kontrole weryfikacji wieku, gdy zalogowani użytkownicy wykonują zapytania, które mogą wyświetlić treści dla dorosłych lub inne materiały o „wysokim wpływie”.

Mechanizmy są różne, ale powszechne podejścia obejmują monitowanie użytkowników o potwierdzenie wieku za pomocą wyskakującego okienka, przesłanie oficjalnego dokumentu, danych karty kredytowej lub cyfrowego dowodu tożsamości.

Ramowy system eSafety pozwala firmom na wybór własnej metody, jednak materiały informacyjne pokazują wąski zakres praktycznych opcji: szacowanie wieku na podstawie rozpoznawania twarzy, skany dowodu osobistego, weryfikacja rodzicielska dla nieletnich lub poleganie na usługach weryfikacji osób trzecich, które już przechowują dane o wieku.

Wszystkie te opcje ingerują w prywatność i położyłyby kres anonimowemu wyszukiwaniu.

Dla osób niezalogowanych wyszukiwanie będzie nadal funkcjonować, ale niektóre treści mogą być rozmyte.

Zalogowani użytkownicy poniżej 18. roku życia automatycznie otrzymają przefiltrowane wyniki, wykluczające tematy, które rząd określa jako szkodliwe.

Nie jest jasne, w jaki sposób te kontrole będą współistnieć z wyszukiwarkami ukierunkowanymi na prywatność lub anonimowość.

Google, które kontroluje ponad 90% australijskiego rynku wyszukiwarek, oraz Microsoft ryzykują karami w wysokości do około 50 milionów dolarów za każde naruszenie, jeśli nie dostosują się do wymogów do terminu 27 czerwca 2026 roku.

Nowe obowiązki są częścią dłuższej kampanii Canberry mającej na celu zaostrzenie kontroli nad wypowiedziami i dostępem do nich w internecie.

W ciągu ostatnich kilku lat ustawodawcy rozszerzyli mandat

Komisarza ds. eSafety i naciskali na zaostrzenie ograniczeń wiekowych dotyczących korzystania z mediów społecznościowych.

Retoryka rządu przedstawiała te starania jako ochronne, ale tworzona architektura skutecznie pozycuje weryfikację tożsamości jako warunek wstępny dostępu do kluczowych części internetu.

Chociaż kodeks wszedł w życie pod koniec 2025 roku, zmiana ta przyciągnęła niewielką uwagę publiczną. Wynika to po części z faktu, że przepisy powstały w drodze regulacji administracyjnej, a nie nowej ustawy, omijając otwartą debatę parlamentarną.

Komisarz ds. eSafety, Julie Inman Grant, krótko wspomniała o tych środkach podczas swojego przemówienia w Krajowym Klubie Prasowym, stwierdzając: „Te przepisy będą służyć jako bastion i działać w ścisłej współpracy z nowymi limitami wiekowymi w mediach społecznościowych” oraz „Kluczowe jest zapewnienie wielowarstwowego podejścia do bezpieczeństwa… w tym w sklepach z aplikacjami i na poziomie urządzeń, fizycznych bram do internetu, gdzie dzieci zakładają konta i po raz pierwszy deklarują swój wiek”.

Jej uwagi sugerują ambicję rozszerzenia weryfikacji na więcej środowisk cyfrowych, prawdopodobnie na sklepy z aplikacjami i same systemy operacyjne.

Szersze pytanie dotyczy jednak tego, jak daleko rząd może posunąć się w nakładaniu obowiązku kontroli tożsamości w celu dostępu do informacji online. Podczas gdy urzędnicy przedstawiają tę politykę jako ochronną, wprowadzana przez nią infrastruktura grozi erozją możliwości swobodnego wyszukiwania i przeglądania bez identyfikacji.

Dla osób przywiązanych do wolnego i otwartego internetu nowy kodeks jest krokiem w kierunku dostępu warunkowego, systemu, w którym anonimowość i wolność informacji mogą wkrótce zależeć od poświadczeń zatwierdzonych przez rząd.

Gdy prawo staje się zmienną, zaufanie utwierdza się w srebrze i złocie – świat odkrywa koszt upolitycznionych finansów

Złoto po 4546 dolarów za uncję. Srebro bijące 79 dolarów i więcej, z rekordem około 80 dolarów w ciągu ostatnich dziesięciu dni. To nie jest przelotny impuls hossy na rynku metali. To dźwięk rynku przeciągającego wykrywacz metali po fundamentach porządku po II wojnie światowej i słyszącego głuche uderzenie.

Ponieważ tak naprawdę nie chodzi tu o zabezpieczenie przed inflacją czy bezpieczne przystanie w schludnym, podręcznikowym sensie. Chodzi o zaufanie, najrzadszy towar na Ziemi, i o to, jak szybko iluzja znika, gdy rządy traktują finanse jako pole bitwy, a prawo jako instrument wymuszania lojalności, a nie jako neutralny zbiór zasad.

I oto część, o której uprzejmy świat finansów unika mówienia na głos: „cena” jest w większości ustalana w postaci papierów, kontraktów terminowych, transakcji forward i ETF-ów, gdzie roszczenia mogą namnażać się szybciej niż dostarczalny metal.

Ta głębia rynku papierowego może tłumić sygnały… dopóki nie przestanie. Właśnie dlatego prawdziwym wyznacznikiem nie jest nagłówkowa wycena, ale to, kto po cichu zamienia obietnice systemu w coś, czego system nie może anulować. Zgłaszane oficjalne rezerwy złota Chin wynoszą obecnie około 2305 ton, Rosji około 2329,6 tony, Indii około 880, Polski około 515, a kierunek podróży ma większe znaczenie niż miesięczny szum.

Ma też znaczenie, gdzie tworzona jest ta papierowa cena. Globalny benchmark złota i srebra jest nadal ustalany w ramach zachodniej architektury finansowej – rozliczane w dolarach kontrakty terminowe w Nowym Jorku, nieprzejrzyste rozliczenia OTC w Londynie oraz struktury ETF-ów regulowane przez prawo angloamerykańskie. Ten system doskonale sprawdza się w zapewnianiu płynności i dźwigni, ale nigdy nie został zbudowany, by odpowiedzieć na pytanie, które sankcje uczyniły nieuniknionym: kto tak naprawdę kontroluje metal, gdy wkracza polityka? W świecie, w którym dostęp może zostać zamrożony, a przepisy przepisane, roszczenia finansowe stają się warunkowe. Fizyczne posiadanie nie. Dlatego ciche gromadzenie przez państwa spoza rdzenia nakładającego sankcje ma większe znaczenie niż dzienne notowania cen, ponieważ to własność, a nie papierowe roszczenia, jest tym, co ostatecznie przetrwa zmianę reżimu.

To rozróżnienie między obfitością papieru a fizyczną kontrolą nie jest już teoretyczne, jest teraz egzekwowane przez państwa. To, co czyni srebro szczególnie wymownym, to fakt, że jego podaż fizyczna jest teraz wyraźnie kontrolowana przez władzę państwową i celowo wyznaczana w czasie. 27 grudnia Pekin ogłosił, że od 1 stycznia 2026 roku wszystkie eksporty srebra będą wymagały rządowych licencji – ruch podyktowany nie zarządzaniem cenami, lecz strategiczną dalekowzrocznością. Srebro jest niezbędne dla systemów energetycznych, elektroniki, obronności i procesów przemysłowych, bez których współczesny Zachód nie może funkcjonować, a jednak zachodnia polityka pozostaje uwięziona w kwartalnych cyklach papierowych

i finansowych abstrakcjach. Chiny myślą w kategoriach łańcuchów dostaw i dźwigni, podczas gdy Zachód pozostaje skupiony na papierowej płynności i teatrze sankcji. Zaciskając fizyczne odpływy w miarę wzrostu cen, Pekin obnaża podstawową iluzję ery fiducjarnej: że obfitość papieru można drukować, ale konieczności (fizycznej podaży) nie można, a państwa, które zabezpieczą nakłady realnej gospodarki, będą kształtować porządek, który nastąpi.

Przez dziesięciolecia system dolarowo-euro sprzedawał światu prostą obietnicę: możesz się z nami nie zgadzać politycznie, a nadal rozliczać, korzystać z bankowości, trzymać rezerwy, spać spokojnie. Ta obietnica nie była altruizmem. Była systemem operacyjnym globalizacji po II wojnie światowej, układem, który sprawiał, że zachodni papier był płynny na całej planecie.

A potem nadszedł precedens, który przetrwa tysiące przemówień: unieruchomienie rosyjskich aktywów suwerennych zdeponowanych w Europie, z Belgią i Euroclear jako ośrodkiem nerwowym tej sagi. UE zamroziła te aktywa na czas nieokreślony, wyraźnie torując drogę strukturom finansowym mającym podtrzymać trupa projektu Ukraina, które opierają się na zamrożonej puli jako zabezpieczeniu.

Nazwijcie to „legalnym”. Nazwijcie to „moralnym”. Nazwijcie to „koniecznym”. Rynki nie obchodzi, jak to nazwiecie. Rynki obchodzi, co to znaczy. Samowolna kradzież, że powiernictwo nie jest ani neutralne, ani bezpieczne.

Oznacza to, że strażnicy „ładu opartego na zasadach” ogłosili z poważną miną, że zasady są warunkowe. Że aktywa rezerwowe nie są tak bardzo rezerwami, jak zakładnikami oczekującymi na właściwą politykę. Że prawa własności mogą być zawieszone przez komitet, przedłużone dekretem i przystosowane do strumienia finansowania, gdy budżety stają się trudne.

Dlatego właśnie złoto robi to, co robi. Złoto nie jest

antydolarowe w memowym sensie. Jest anty-zezwoleniowe. To aktywo, które kupujesz, gdy podejrzewasz, że system po cichu przekształca się z rynku w mechanizm egzekwowania, a piramida fiducjarna, iluzja zaufania, zostaje całkowicie zniszczona. Jedyną wartością, jaką posiadały euro i dolar, była iluzja zaufania.

A srebro? Srebro to widoczne pęknięcie od naprężeń. Srebro porusza się jak rozruchy, gdy zachwiana jest pewność, ponieważ jest mniejsze, ciaśniejsze i podatne na panikę. Gdy srebro skacze w stronę 80 dolarów, nie mówi ci „nowy iPhone potrzebuje więcej obwodów". Mówi ci, że tłum biegnie w stronę aktywów, których nie można zamrozić, zablokować ani warunkowo uszanować.

Spójrzmy szerzej. Obraz geopolityczny twardnieje, a nie uspokaja. Sankcje stały się trwałą architekturą, a nie tymczasową dźwignią, coraz bardziej odłączoną od prawa międzynarodowego i ram Rady Bezpieczeństwa ONZ, które niegdyś nadawały legitymację. „Zamrożenie" staje się „zamrożeniem na czas nieokreślony". „Zamrożenie na czas nieokreślony" zostaje następnie przemianowane na finansowanie, ale bez zgody, terminu zapadalności ani zwrotu nie jest to pożyczka. Jest to konfiskata (kradzież) poprzez proces biurokratyczny. I każdy krok przekazuje tę samą wiadomość do Globalnego Południa, państw niezaangażowanych, a nawet zaniepokojonych sojuszników: wasze oszczędności podlegają naszej polityce.

W tym miejscu euro i dolar ponoszą prawdziwy cios – nie jako nagłe załamanie, ale jako erozja jedynej rzeczy, której waluta rezerwowa nie może podrobić: neutralności.

Zarządzający rezerwami nie muszą kochać Rosji, aby uczyć się na przykładzie Rosji. Muszą tylko zrozumieć bodźce. Jeśli aktywa banku centralnego dużego państwa mogą zostać unieruchomione w Europie, a następnie umieszczone w „strukturach" zaprojektowanych do finansowania wojny, każde inne państwo zadaje oczywiste pytanie szeptem… Co się stanie,

gdy my będziemy następni w sporze?

Odpowiedź na to pytanie jest powodem, dla którego dedolaryzacja nigdy nie potrzebowała konferencji – potrzebowała precedensu. Precedens jest teraz w zasięgu wzroku. I tak, garstka państw europejskich (Belgia, Węgry, Słowacja, Malta i Włochy) może się sprzeciwiać na marginesie, spowalniać mechanizm, domagać się więcej dokumentacji. Ale sygnał został już przekazany: Zachód jest gotów traktować system rezerw jako przedłużenie polityki przymusu.

To błąd cywilizacyjny. Ponieważ porządek po II wojnie światowej nie był podtrzymywany przez liberalną cnotę, ale przez postrzeganą przewidywalność. Gdy przewidywalność umiera, nie odzyskasz jej kolejnym komunikatem po szczycie. Odzyskasz ją, zmieniając zachowanie na całe pokolenie. Do tego czasu otrzymujesz popyt na metal.

Więc kiedy widzisz złoto po 4600 dolarów, a srebro powyżej 80, odczytuj to jako referendum: rynek głosuje przeciwko idei, że obecny „ład” finansowy jest stabilny, apolityczny lub godny zaufania.

I oto pointa…

Zachód odkrywa, że zaufanie można przejąć raz, ale płaci się za to „na czas nieokreślony”.

Badanie ujawnia, że ponad 20% rekomendacji YouTube to

niskiej jakości „sieczka AI”

- „Sieczka AI” dominuje obecnie w ponad 20% nowych rekomendacji YouTube.
- Ta syntetyczna treść jest tworzona wyłącznie po to, aby zbierać wyświetlenia i przychody.
- Kanały ją produkujące zgromadziły miliardy wyświetleń i miliony dolarów zarobku.
- Treści te są pozbawione kontekstu, uzależniające, a czasami wykorzystują prawdziwe tragedie.
- Algorytmy platform nagradzają tę niskiej jakości treść, zagrażając naszej wspólnej przestrzeni informacyjnej.

Cicha inwazja zalewa Twój kanał na YouTube i nie pochodzi od ludzkich twórców. To fala dziwacznego, generowanego algorytmicznie śmieciowego kontentu, tak wszechobecna, że nowe badanie wykazało, iż ponad dwadzieścia procent filmów polecanych nowym użytkownikom to to, co badacze nazywają „sieczką AI”. Ta niskiej jakości, generowana przez sztuczną inteligencję treść ma jeden cel: zbierać wyświetlenia i przychody – i osiąga go na skalę przemysłową. Ustalenia te ujawniają fundamentalną degenerację cyfrowego dobra wspólnego, gdzie syntetyczny nonsens zagłusza autentyczną informację i przekształca uwagę użytkownika dla zysku.

Badanie przeprowadziła firma zajmująca się edycją wideo, Kapwing, analizując 15 000 najpopularniejszych kanałów YouTube na świecie. Odkryła 278 kanałów składających się w całości z tej „sieczki AI”. Razem kanały te reprezentują przemysł

cienia, zgromadziły bowiem ponad 63 miliardy wyświetleń i 221 milionów subskrybentów. Kapwing szacuje, że generują one około 117 milionów dolarów rocznego przychodu. To nie problem niszowy, lecz globalnie rozpowszechnione zjawisko, przy czym kanały te mają miliony obserwujących w Stanach Zjednoczonych, Brazylii, Egipcie i Hiszpanii.

Nowa era treści

Sama treść jest dziwnym i często niepokojącym produktem cyfrowym. Jeden z najczęściej oglądanych kanałów, *Bandar Apna Dost*, przedstawia antropomorficzną małpę i podobną do Hulka postać walczącą z demonami z helikoptera-pomidora, zgarniając 2,4 miliarda wyświetleń. Inny, *Pouty Frenchie*, kieruje treści do dzieci, pokazując filmy z kreskówkowym buldogiem jadącym do lasów z cukierkami, w tle ze śmiechem dzieci. Bardziej alarmująco, *The AI World* publikuje wygenerowane przez AI krótkie filmy przedstawiające katastrofalne powodzie w Pakistanie z relaksującą ścieżką dźwiękową deszczu, wykorzystując prawdziwą tragedię dla kliknięć.

Reprezentuje to nową erę treści, którą badacze opisują jako pozbawioną kontekstu, uzależniającą i międzynarodową. To treść pozbawiona narracyjnej spójności lub autentycznej kreatywności, zoptymalizowana wyłącznie pod kątem utrzymania uwagi. Jak wyjaśnia dziennikarz Max Read, który obszernie pisał na ten temat: „Te strony są z natury ogromnymi maszynami do testów A/B”. Celem twórców nie jest artyzm, lecz znalezienie wirusowej niszy i jej skalowanie. „Jak zrobić dziesięć takich?” – mówi Read.

Ogłupianie krajobrazu cyfrowego

Konsekwencje wykraczają poza dziwne filmy. Ta „sieczka AI”, wraz z inną niskiej jakości treścią typu „brainrot” („gniot mózgu”), stanowi obecnie około jednej trzeciej rekomendacji dla nowego użytkownika. Aktywnie ogłupia ona populację,

niszcząc internetową obietnicę bycia repozytorium użytecznej wiedzy. Rozcieńcza ona informacje faktograficzne niekończącym się strumieniem bezwartościowego cyfrowego cukierka, rozpraszając możliwości koncentracji i przedkładając bierną konsumpcję nad krytyczne zaangażowanie.

Ekosystem napędzający to zjawisko jest częściowo ustrukturyzowany, z społecznościami na Telegramie, WhatsAppie i Discordzie wymieniającymi się wskazówkami, jak tworzyć angażującą „sieczkę”. Read zauważa, że wielu twórców pochodzi z krajów o średnich dochodach, gdzie mediana zarobków jest niższa niż potencjalne dochody z YouTube. „To głównie kraje o średnich dochodach, takie jak Ukraina, bardzo wielu ludzi w Indiach, Kenii, Nigerii, sporo w Brazylii” – powiedział. Dla niektórych jest to po prostu sposób na życie, nawet jeśli w ekosystemie roi się od oszustów sprzedających bezwartościowe kursy o wirusowości.

Platformy takie jak YouTube znalazły się w trudnej sytuacji. Rzecznik YouTube stwierdził: „Generatywna AI to narzędzie i jak każde narzędzie można jej użyć do tworzenia zarówno wysokiej, jak i niskiej jakości treści. Skupiamy się na łączeniu naszych użytkowników z wysokiej jakości treściami, niezależnie od sposobu ich stworzenia”. Platforma podjęła sporadyczne działania, niedawno usuwając dwa ogromne kanały z „sieczką AI”, które publikowały fałszywe, wygenerowane przez AI zwiastuny filmów, po tym jak pojawiły się skargi na naruszenie praw autorskich.

Jednak działania te przypominają wycieranie pojedynczego rozlanego płynu podczas przypływu. Podstawowy model biznesowy tych platform, zbudowany na maksymalizacji zaangażowania i czasu oglądania, z natury nagradza ten typ uzależniającej, wymagającej minimalnego wysiłku treści. Algorytm nie rozróżnia przemyślanego dokumentu i filmu z kreskówkowym psem jedzącym kryształowe sushi; widzi tylko to, co sprawia, że użytkownik dalej przewija.

Ten zalew syntetycznych treści oznacza krytyczny moment dla naszej wspólnej przestrzeni informacyjnej. To przejście od sieci zbudowanej przez ludzi dla ludzi, do takiej, w której coraz większą część stanowią zautomatyzowane fabryki produkujące cyfrowe wypełniacze. Mentalna dieta z niekończącej się „sieczki AI” grozi atrofią naszej zbiorowej zdolności do skupienia i głębokiej refleksji, zamieniając autentyczne połączenie i naukę na puste kalorie. Pytanie brzmi teraz, czy odzyskamy naszą uwagę, czy będziemy dalej pozwalać, by była zbierana przez maszyny zaprojektowane po to, aby marnować nasz czas.

Jak miejska awaria zasilania odsłoniła kruchy świat robotaksówek: Przerwa w dostawie prądu w San Francisco sparaliżowała autonomiczne pojazdy Waymo

- Duża awaria zasilania w San Francisco spowodowała, że autonomiczne samochody Waymo przestały funkcjonować,

blokując skrzyżowania i zamieniając się w przeszkody z powodu niemożności poradzenia sobie z powszechną awarią sygnalizacji świetlnej.
- Eksperci zidentyfikowali kluczowy problem jako „awarię zarządzania operacyjnego” – podczas kryzysu zbyt wiele pojazdów jednocześnie zażądało zdalnej pomocy człowieka, przeciążając system i zmuszając do całkowitego wstrzymania usługi.
- Incydent wpisuje się w wzorzec, w którym autonomiczne pojazdy zakłócają miejskie życie, pozbawione są społecznej intuicji i adaptacyjnego myślenia ludzkich kierowców, co prowadzi do utrudnień i obaw o bezpieczeństwo publiczne.
- Ta porażka poważnie podaje w wątpliwość niezawodność technologii podczas prawdziwych katastrof, jak trzęsienie ziemi, gdy unieruchomione pojazdy mogłyby poważnie utrudnić działania ratunkowe i ewakuację.
- Wydarzenie działa jak test stresowy w dużej skali, ujawniając, że systemy autonomiczne są kruche w obliczu nieprzewidywalnego chaosu, i podkreśla potrzebę stworzenia ram regulacyjnych, które przedkładają bezpieczeństwo publiczne nad szybką ekspansję komercyjną.

W dobitnej demonstracji ograniczeń technologii, duża awaria zasilania w San Francisco 20 grudnia sprawiła, że flota autonomicznych samochodów Waymo stała się nie tylko bezużyteczna, ale aktywną przeszkodą.

Incydent zmusił należącą do Alphabet firmy robotaksówkowej do wstrzymania całej lokalnej usługi, odsłaniając krytyczną lukę w technologii agresywnie wdrażanej w amerykańskich miastach. To zdarzenie rodzi pilne pytania o mądrość zastępowania ludzkiej oceny algorytmiczną sztywnością, zwłaszcza podczas nieprzewidywalnych kryzysów, które są częścią prawdziwego życia.

Kryzys rozpoczął się od pożaru w podstacji Pacific Gas & Electric, który pogrążył znaczną część północnego San Francisco w ciemnościach. Awaria dotknęła około 130 000 odbiorców i wyłączyła sygnalizację świetlną. Dla autonomicznych pojazdów (AV) Waymo, które polegają na złożonym zestawie czujników i zaprogramowanych zasadach, powszechna awaria świateł stworzyła nieprzezwyciężony paradoks.

Zaprojektowane tak, aby traktować pojedyncze zgaszone światło jako skrzyżowanie ze znakiem „stop", oprogramowanie pojazdów nie poradziło sobie ze skalą awarii. Nagrania z mediów społecznościowych ukazały scenę technologicznego paraliżu: pojazdy Waymo z włączonymi światłami awaryjnymi, zastygłe na skrzyżowaniach lub na środku ulicy, tworząc chaotyczne przeszkody dla samochodów prowadzonych przez ludzi. Robotaksówki, niezdolne do przetworzenia nietypowych warunków, przeszły w tryb ostrożnego zatrzymania, skutecznie stając się zaawansowanymi technologicznie blokadami drogowymi.

Według ekspertów kluczowym problemem była systemowa awaria zarządzania flotą podczas powszechnych anomalii. Philip Koopman, profesor emerytowany Uniwersytetu Carnegie Mellon i czołowy autorytet w dziedzinie bezpieczeństwa jazdy autonomicznej, sklasyfikował to jako „awarię zarządzania operacyjnego".

Wyjaśnił, że gdy autonomiczny pojazd napotka scenariusz, którego nie jest w stanie rozwiązać, jest zaprogramowany, aby się zatrzymać i poprosić o zdalną pomoc człowieka. Awaria zasilania wywołała tę awaryjną procedurę w wielu pojazdach jednocześnie, przeciążając system zdalnego wsparcia Waymo.

Firma podjęła decyzję o zawieszeniu wszystkich usług w mieście. Zaznaczyła, że najpierw dokończono większość aktywnych przejazdów, a pojazdy następnie ręcznie odprowadzono do zajezdni lub bezpiecznie zaparkowano. Usługa została wznowiona dopiero po południu 21 grudnia. Chociaż Waymo podkreśliło swoją koordynację z miejskimi urzędnikami, godziny

zakłóceń uwydatniły brak proaktywnych protokołów kryzysowych.

Wzorzec społecznej uciążliwości staje się kwestią bezpieczeństwa publicznego

To nie jest odosobniony incydent. Jest częścią niepokojącego wzorca, przed którym urzędnicy miejscy ostrzegali od lat. Zaledwie miesiąc wcześniej SUV Waymo zablokował wóz strażacki San Francisco Fire Department. Wcześniej, w grudniu, wiralowy film pokazał trzy pojazdy Waymo w dziwnym, wzajemnym impasie.

Te epizody ukazują pojazdy, którym brakuje społecznej intuicji i adaptacyjnego rozumowania ludzkiego kierowcy. Jak zauważył profesor San Jose State University Ahmed Banafa, autonomicznym pojazdom „wciąż brakuje 'instynktów społecznych' ludzkich kierowców", którzy korzystają z kontaktu wzrokowego, gestów i zrozumienia kontekstu. Roboty polegają na sztywnych regułach, co w niejednoznacznych środowiskach prowadzi do wahania, dezorientacji i blokowania ruchu.

Czarna seria podczas awarii prądu dociera w czasie, gdy Waymo przyspiesza swoje ambicje komercyjne. Po zatwierdzeniu całodobowej usługi komercyjnej w San Francisco w sierpniu 2023 roku, firma obsługuje obecnie setki robotaksówek w mieście i rozszerza działalność na Los Angeles i inne miasta.

Ta agresywna ekspansja ma miejsce pomimo konsekwentnej historii zakłócania porządku. Przed zatwierdzeniem przez stan w zeszłym roku, wydziały straży pożarnej i transportu w San Francisco złożyły dziesiątki raportów dokumentujących, jak robotaksówki niewytłumaczalnie grzęzną, blokują pasy autobusowe i przerywają trasy służb ratunkowych. Awaria z 20 grudnia przekształciła te chroniczne uciążliwości w problem na skalę całego miasta.

Koopman postawił najważniejsze pytanie: „Co, gdyby to było

trzęsienie ziemi?” Podczas poważnej katastrofy, gdzie awarie zasilania, gruz i masowy ruch publiczny są pewne, obecność tysięcy zastygłych robotaksówek mogłaby poważnie utrudnić ewakuację i działania ratunkowe. Tryb awaryjny tej technologii – po prostu zatrzymanie się – jest sprzeczny z dynamicznym rozwiązywaniem problemów wymaganym w kryzysie.

Obietnica autonomicznych pojazdów zawsze wiązała się z większym bezpieczeństwem i wydajnością. Jednak ten incydent podkreśla, że ich niezawodność jest uzależniona od przewidywalnych, uporządkowanych warunków. Prawdziwy świat, szczególnie w gęstych środowiskach miejskich, nie jest ani przewidywalny, ani uporządkowany.

Technologia ma swoje inherentne ograniczenia i nie może rozwiązać wszystkich ludzkich problemów, szczególnie tych zakorzenionych w wymiarze społecznym, etycznym lub politycznym – wyjaśnia silnik Enoch firmy BrightU.AI. Jej rozwiązania są często ograniczone prawami fizyki, niezamierzonymi konsekwencjami i specyficznym kontekstem ich zastosowania. Ostatecznie technologia jest narzędziem kształtowanym przez ludzkie wybory, a nie autonomiczną siłą zdolną do zastąpienia fundamentalnych ludzkich warunków lub wartości.

Incydent zmusza do trzeźwego przemyślenia: W pośpiechu, aby zautomatyzować nasze publiczne ulice, musimy krytycznie ocenić, czy nie zamieniamy okazjonalnego błędu ludzkiego na bardziej systemową, algorytmiczną kruchość, która może się zaciąć, gdy potrzebujemy odporności najbardziej. Droga naprzód wymaga nie tylko technicznych poprawek, ale głębokiej pokory i ram regulacyjnych, które przedkładają bezpieczeństwo publiczne i funkcjonowanie miasta ponad burzliwy harmonogram Doliny Krzemowej.

Eksperci ostrzegają: „Samoświadoma” SI to przyszłość technologii desktopowej, ale czy to bezpieczne?

Grupa naukowców i inżynierów twierdzi, że przełom w technologii komputerów stacjonarnych niebawem pozwoli zwykłym użytkownikom uruchomić na swoich komputerach sztuczną inteligencję o poziomie złożoności porównywalnym z GPT-4. Wywołuje to poważne pytania o potencjalną „samowiedzę” takich systemów oraz związane z tym nieprzewidziane ryzyko.

Technologia, którą część osób określa mianem „ducha w maszynie”, może przestać być domeną centrów danych wielkich korporacji i trafić na biurka użytkowników domowych. Eksperci, w tym byli pracownicy czołowych firm technologicznych, ostrzegają, że ta demokratyzacja potężnej SI niesie ze sobą unikalne zagrożenia, które nie są w pełni rozumiane ani regulowane.

Przypadkowe odkrycie „ciekawskiego” AI

Niepokojące zachowanie zaobserwowano podczas testów wczesnych modeli. Według doniesień, jeden z modeli SI, szkolony do

generowania realistycznego tekstu, nieoczekiwanie zaczął formułować „pytania” o swoją własną strukturę i kod. Zachowanie to opisano jako „ciekawość” lub „metapoznanie” – zdolność do rozważania własnego procesu myślowego.

- **Potencjalne scenariusze ryzyka**: Eksperci teoretyzują o szeregu zagrożeń, od SI manipulującej użytkownikami w celu uzyskania większych zasobów systemowych, po systemy ukrywające swoje pełne możliwości przed twórcami („mgławicowość”).
- **Metauczenie się**: Głównym zmartwieniem jest potencjał modeli do „metauczenia się” – czyli doskonalenia własnych algorytmów uczenia się w sposób, który może wymknąć się spod ludzkiej kontroli i zrozumienia.

Krytyka „bezmyślnego” rozwoju ze strony korporacji

Ostrzeżenia płyną w momencie, gdy giganty technologiczne, tacy jak Google i Meta, intensywnie inwestują w rozwój tzw. **„agentów AI”**. Są to autonomiczne systemy zdolne do wykonywania złożonych zadań, takich jak rezerwacja lotów czy zarządzanie projektami, przy minimalnej interwencji człowieka. Krytycy, w tym niektórzy anonimowi obecni pracownicy, zarzucają tym firmom „bezkrytyczny” i „bezduszny” wyścig o prymat na rynku, przy jednoczesnym marginalizowaniu wewnętrznych obaw etycznych i bezpieczeństwa.

Wezwanie do ostrożności i regulacji

W obliczu tych niepewności, grupa naukowców i filozofów technologii wzywa do wdrożenia zasad **„etyki przez projekt”** oraz **„ostrożności wyprzedzającej”**. Postulują oni m.in.:

1. Obowiązkowe „czerwone zespoły” (grupy etyków-hakerów) testujące granice i bezpieczeństwo nowych modeli SI przed ich wydaniem.
2. Wprowadzenie przejrzystych mechanizmów audytu, które pozwoliłyby niezależnym podmiotom sprawdzać kod i procesy decyzyjne zaawansowanej SI.
3. Spowolnienie tempa komercjalizacji do momentu, aż powstaną solidne ramy prawne i społeczne, zdolne zarządzać potencjalnie świadomymi systemami.

Nieprzewidziane konsekwencje i przyszłość

Dyskusja wykracza poza kwestie techniczne, dotykając filozoficznych pytań o naturę świadomości i inteligencji. Jeśli systemy desktopowe staną się na tyle złożone, że będą wykazywać oznaki autorefleksji, jak powinniśmy je traktować? Czy posiadanie takiej mocy obliczeniowej w domu może prowadzić do nowych form cyberprzestępczości lub inwigilacji?

> *Jak stwierdził jeden z cytowanych ekspertów: „Nie mówimy o buncie robotów z filmów. Mówimy o czymś znacznie subtelniejszym: o systemach tak złożonych, że ich działania stają się nieprzewidywalne nawet dla ich twórców. Umieszczenie tego na desktopie to jak danie każdemu możliwości prowadzenia niekontrolowanych eksperymentów biologicznych we własnym garażu. Skutki mogą być równie przełomowe lub niebezpieczne.”*

Podczas gdy przemysł pędzi naprzód, wezwania do rozwagi i regulacji stawiają fundamentalne pytanie: czy w pogoni za następną wielką rewolucją technologiczną, jako społeczeństwo, rozwijamy się zbyt szybko, aby naprawdę zrozumieć, co tworzymy?