Globalny traktat dotyczący cyberprzestępczości spotyka się z krytyką organizacji praw człowieka i firm technologicznych w związku z obawami dotyczącymi inwigilacji

Sześćdziesiąt pięć krajów, w tym Stany Zjednoczone i Kanada, podpisało traktat ONZ dotyczący cyberprzestępczości, który zagraża prywatności, badaniom online i wolności słowa.

Umowa, znana jako Konwencja ONZ o cyberprzestępczości, została podpisana w Hanoi i wejdzie w życie po ratyfikacji przez 40 państw członkowskich.

Każdy kraj musi przeprowadzić własny proces ratyfikacji. W Stanach Zjednoczonych do zatwierdzenia porozumienia wymagana jest zgoda dwóch trzecich głosów w Senacie.

Sekretarz generalny ONZ António Guterres opisał traktat jako niezbędny krok w walce z cyberprzestępczością, stwierdzając, że „cyberprzestrzeń stała się podatnym gruntem dla przestępców… każdego dnia wyrafinowane oszustwa pozbawiają rodziny środków do życia, kradną im źródła utrzymania i wyczerpują nasze gospodarki miliardami dolarów”.

Nazwał konwencję „potężnym, prawnie wiążącym instrumentem wzmacniającym naszą zbiorową obronę przed cyberprzestępczością” i podkreślił, że „nie może ona być wykorzystywana do jakichkolwiek form nadzoru lub innych działań, które mogłyby być powiązane z naruszeniami praw człowieka”.

Biuro Narodów Zjednoczonych ds. Narkotyków i Przestępczości (UNODC), które kierowało negocjacjami, argumentowało, że traktat zawiera zabezpieczenia dotyczące praw człowieka i legalnych badań naukowych.

Jednak organizacje takie jak Human Rights Watch (HRW) i Electronic Frontier Foundation (EFF) nie zgadzają się z tym stanowiskiem.

Przed podpisaniem traktatu obie organizacje wezwały rządy do niepopierania go, ostrzegając, że jego niejasne definicje mogą pozwolić rządom na monitorowanie obywateli, ściganie badaczy zajmujących się bezpieczeństwem i tłumienie wypowiedzi politycznych.

Obawy zgłosiły również firmy technologiczne. Porozumienie Cybersecurity Tech Accord, którego członkami są m.in. Meta i Microsoft, określiło traktat jako „traktat o inwigilacji”, który może promować wymianę danych przez rządy i kryminalizować etyczne hakowanie.

Wietnam, gospodarz ceremonii podpisania traktatu, spotkał się z wielokrotną krytyką za cenzurę internetową. Departament Stanu USA wspomniał ostatnio o „poważnych problemach związanych z prawami człowieka” w tym kraju, a organizacja Human Rights Watch informuje, że w tym roku co najmniej 40 osób zostało aresztowanych za działalność w Internecie.

Prezydent Wietnamu Luong Cuong z zadowoleniem przyjął traktat, mówiąc, że „nie tylko oznacza on narodziny globalnego instrumentu prawnego, ale także potwierdza trwałą żywotność multilateralizmu, w ramach którego kraje pokonują różnice i są

gotowe wspólnie ponosić odpowiedzialność za wspólne interesy pokoju, bezpieczeństwa, stabilności i rozwoju”.

Zwolennicy twierdzą, że porozumienie poprawi koordynację działań przeciwko przestępstwom takim jak oprogramowanie ransomware, phishing i handel internetowy. Przeciwnicy utrzymują, że szerokie postanowienia traktatu mogą umożliwić rządom nadużywanie przepisów dotyczących cyberprzestępczości w celu ścigania dziennikarzy, badaczy i aktywistów.

Podpisanie konwencji o cyberprzestępczości następuje w momencie, gdy Guterres nadal rozszerza swoje wezwanie do globalnych działań przeciwko temu, co określa jako „dezinformację i fałszywe informacje” oraz „nękanie w Internecie”.

Przemawiając na **konferencji Światowej Organizacji Meteorologicznej w Genewie**, Guterres powiązał rozpowszechnianie „fałszywych” informacji z publicznym zamieszaniem wokół zmian klimatycznych i wezwał rządy do „przeciwstawiania się fałszywym narracjom” oraz ochrony badań naukowych przed zniekształcaniem.

„Musimy walczyć z dezinformacją, nękaniem w Internecie i greenwashingiem” – powiedział delegatom.

Ukryte koszty energii wiatrowej: nowe badania ujawniają katastrofalny wpływ

na populacje ptaków i nietoperzy

- Turbiny wiatrowe zabijają co roku setki tysięcy, a nawet miliony nietoperzy i ptaków na całym świecie. W samych Stanach Zjednoczonych każdego roku ginie 500 000 nietoperzy, co jest porównywalne z liczbą ptaków morskich, które zginęły w wyniku wycieku ropy z platformy Deepwater Horizon. Zagrożone gatunki, takie jak orły przednie, sępy płowe i nietoperze siwe, są narażone na lokalne wyginięcie.
- Turbiny zmieniają zachowanie zwierząt, mikroklimat i zdrowie gleby, zmniejszając populacje dżdżownic i roślinność. W Chinach pojedyncza turbina wiatrowa zmniejsza liczebność ptaków o 9,75% i bogactwo gatunkowe o 12,2%. Prawie 50% badanych gatunków ptaków w Kalifornii wykazało spadek populacji związany z turbinami.
- Zwolennicy energii wiatrowej twierdzą, że zmiany klimatyczne stanowią większe zagrożenie, ale działania łagodzące (unikanie lokalizacji, środki odstraszające) pozostają niespójne i niesprawdzone na dużą skalę. Istnieją polityki rekompensaty siedlisk, ale nie są one w stanie zrównoważyć szkód ekologicznych na dużą skalę.
- Chociaż turbiny powodują mniejszą liczbę zgonów ptaków na gigawatogodzinę niż paliwa kopalne (1,31 w porównaniu z 5,2 dla węgla), ich szybka ekspansja zagraża ekosystemom. Proponowane farmy wiatrowe zajmujące 13

procent powierzchni Stanów Zjednoczonych mogą mieć „dramatyczne konsekwencje dla różnorodności biologicznej”.
- Pilnie potrzebne jest strategiczne rozmieszczenie, rygorystyczne oceny środowiskowe i inwestycje w mniej szkodliwe odnawialne źródła energii. Polityka zerowej emisji netto nie może poświęcać ekosystemów – „zielona” etykieta energii wiatrowej ignoruje jej niszczycielski wpływ na dziką przyrodę.

Seria przełomowych badań ujawniła alarmujące szkody ekologiczne spowodowane przez lądowe turbiny wiatrowe, rodząc pilne pytania o prawdziwą zrównoważoność rozwoju energii odnawialnej.

*BrightU.AI’*s Enoch wyjaśnia, że lądowe turbiny wiatrowe, znane również jako turbiny naziemne lub lądowe, są rodzajem konwertera energii wiatrowej, który wytwarza energię elektryczną z energii kinetycznej wiatru. Zazwyczaj są one instalowane na lądzie, na różnych wysokościach i w różnych lokalizacjach geograficznych, w zależności od zasobów wiatru i połączeń sieciowych.

Chociaż energia wiatrowa jest promowana jako kluczowe rozwiązanie w walce ze zmianami klimatycznymi, nowe badania pokazują, że jej wpływ na różnorodność biologiczną – zwłaszcza populacje ptaków i nietoperzy – może być znacznie poważniejszy niż wcześniej sądzono.

Szokujący raport opublikowany w zeszłym miesiącu w czasopiśmie „Nature” – w dużej mierze zignorowany przez media głównego nurtu – szczegółowo opisuje, w jaki sposób turbiny wiatrowe zakłócają ekosystemy, zabijają dzikie zwierzęta i fragmentują siedliska.

Badanie, przeprowadzone przez międzynarodowy zespół ekologów, ostrzega, że elektrownie wiatrowe „mogą mieć poważne i nieoczekiwane konsekwencje dla różnorodności biologicznej”,

wpływając na gatunki od owadów po drapieżniki szczytowe.

Masowe śmiertelność dzikich zwierząt

Dane są zatrważające:

- W krajach o dużej gęstości turbin co roku ginie nawet milion nietoperzy.
- W samych Stanach Zjednoczonych ginie 500 000 nietoperzy rocznie – liczba ta jest niemal równa szacowanej liczbie 600 000 ptaków morskich zabitych w wyniku wycieku ropy z platformy BP Deepwater Horizon.
- W Wielkiej Brytanii ginie 30 000 nietoperzy rocznie, w Kanadzie 50 000, a w Niemczech 200 000.
- Duże ptaki drapieżne, w tym orły przednie, są zagrożone lokalnym wyginięciem z powodu kolizji z turbinami.

„Być może największą niewiadomą w przewidywaniu przyszłego wpływu energii wiatrowej na różnorodność biologiczną jest zakres potencjalnego rozwoju tej technologii i skumulowane konsekwencje tego rozwoju dla gatunków i ekosystemów” – ostrzega badanie opublikowane w czasopiśmie „Nature”.

Kaskadowe zakłócenia ekosystemu

Oprócz bezpośrednich ofiar śmiertelnych turbiny wiatrowe zmieniają zachowanie zwierząt, ich fizjologię i integralność siedlisk. Profesor Christian Voigt, jeden z autorów badania, ostrzegał wcześniej, że śmiertelność owadów spowodowana przez turbiny może przyczynić się do wyginięcia gatunków. Jego badania z 2022 r. wykazały, że turbiny zmieniają mikroklimat i zmniejszają populację dżdżownic, pogarszając jakość gleby i roślinności.

Raport podkreśla spadek populacji gatunków wrażliwych:

- Sępy płowe i sępy płowe w Europie są zagrożone

wyginięciem.
- Populacja nietoperzy siwych w Ameryce Północnej i błotniaków czarnych w Afryce Południowej maleje.
- Prawie 50 procent gatunków ptaków badanych w Kalifornii wykazało spadek populacji związany z turbinami.

W Chinach, gdzie moc energii wiatrowej jest największa na świecie, ostatnie badania wykazały, że wzrost liczby turbin o jedno odchylenie standardowe (około 84 jednostki) spowodował spadek liczebności ptaków o 9,75 procent i bogactwa gatunkowego o 12,2 procent. Najbardziej ucierpiały ptaki wędrowne oraz te żyjące w lasach, na terenach rolniczych i obszarach miejskich.

Reakcja branży i działania łagodzące

Zwolennicy energii wiatrowej twierdzą, że zmiany klimatyczne stanowią większe zagrożenie dla różnorodności biologicznej niż turbiny. Brytyjska organizacja Bat Conservation Trust stwierdza: „Potrzebujemy energooszczędnych budynków i energii odnawialnej, aby złagodzić zmiany klimatyczne z korzyścią dla nietoperzy, ludzi i środowiska naturalnego”.

Jednak strategie łagodzące – takie jak unikanie wrażliwych obszarów, odstraszanie dzikich zwierząt i rekompensata za utratę siedlisk – pozostają niespójne w skali globalnej. W badaniu opublikowanym w czasopiśmie „Nature” zauważono, że chociaż środki te są pomocne, ich skuteczność nie została „sprawdzona” w kontekście ekspansji farm wiatrowych na dużą skalę.

Redukcja emisji dwutlenku węgla a utrata różnorodności biologicznej

Pomimo szkód ekologicznych, korzyści płynące z energii wiatrowej w zakresie redukcji emisji dwutlenku węgla są niezaprzeczalne. Badania pokazują, że turbiny wiatrowe

powodują znacznie mniejszą liczbę śmiertelnych wypadków ptaków na gigawatogodzinę niż paliwa kopalne (1,31 śmierci/GWh w porównaniu z 5,2 w przypadku węgla). W Chinach korzyści ekonomiczne wynikające z redukcji emisji dwutlenku węgla przewyższają straty w zakresie różnorodności biologicznej w porównaniu z energią wytwarzaną z węgla.

Jednak krytycy twierdzą, że polityka zerowej emisji netto przedkłada cele energetyczne nad ochronę środowiska. Artykuł w czasopiśmie „Nature" ostrzega, że przeznaczenie 13% powierzchni Stanów Zjednoczonych na farmy wiatrowe – zgodnie z propozycją zawartą w raporcie z 2021 r. – może mieć „dramatyczne konsekwencje dla różnorodności biologicznej".

Wezwanie do zrównoważonej polityki energetycznej

W obliczu wyścigu narodów o dekarbonizację badania te podkreślają potrzebę strategicznego rozmieszczenia farm wiatrowych, rygorystycznych ocen środowiskowych i inwestycji w mniej szkodliwe odnawialne źródła energii. Pozostaje pytanie: czy możemy osiągnąć cele klimatyczne bez poświęcania niezastąpionych ekosystemów?

Na razie nauka jest jasna – energia wiatrowa nie jest tak „zielona", jak się ją reklamuje. Prawdziwą cenę zerowej emisji dwutlenku węgla można zapłacić krwią: krwią nietoperzy, ptaków i delikatnej sieci życia, którą podtrzymują.

Czerwony ekran śmierci:

automatyczny atak Google na konkurenta, którego nie udało się przejąć

- Usługa Bezpieczne przeglądanie Google błędnie oznaczyła całą domenę immich.cloud, na której znajduje się samodzielnie hostowana platforma fotograficzna Immich, jako „niebezpieczną”.
- Automatyczna blokada wyświetlała poważne czerwone ekrany ostrzegawcze, skutecznie uniemożliwiając użytkownikom i programistom dostęp do własnych usług.
- Zaznaczone adresy URL były wewnętrznymi środowiskami testowymi i podglądowymi dla projektu Immich, a nie złośliwymi witrynami przeznaczonymi do phishingu lub oszustw.
- Pomimo pomyślnego odwołania blokada została automatycznie przywrócona, zmuszając zespół Immich do migracji swoich systemów do nowej domeny, aby uniknąć dalszych zakłóceń.
- Incydent ten podkreśla znaczną władzę, jaką pojedyncza korporacja ma nad dostępnością sieci, i budzi obawy dotyczące systemowego uprzedzenia wobec niezależnego oprogramowania skupionego na prywatności.

W ramach działania, które podkreśla niebezpieczeństwa związane ze scentralizowaną kontrolą nad internetem, automatyczne systemy bezpieczeństwa Google niedawno błędnie zidentyfikowały

Immich, znaną alternatywę dla Google Photos, jako niebezpieczny podmiot. Incydent, który miał miejsce w październiku 2025 r., spowodował, że usługa Bezpieczne przeglądanie Google zablokowała dostęp do całej domeny immich.cloud, wyświetlając poważne ostrzeżenia, skutecznie dławiąc usługę zaprojektowaną, aby oferować użytkownikom ucieczkę od korporacyjnego gromadzenia danych. Dla zwolenników prywatności i rosnącej liczby użytkowników rozczarowanych wielkimi firmami technologicznymi błędne oznaczenie legalnego projektu open source stanowi surowe przypomnienie o władzy, jaką posiada pojedyncza firma, dyktując, co jest bezpieczne i dostępne w otwartej sieci.

Automatyczny strażnik zawodzi

Usługa Bezpieczne przeglądanie Google jest zintegrowana z głównymi przeglądarkami internetowymi, w tym Chrome i Firefox, gdzie działa jako automatyczny strażnik przed złośliwymi stronami internetowymi. Jego celem jest ochrona użytkowników przed oszustwami phishingowymi i złośliwym oprogramowaniem. Jednak w tym przypadku system wziął na celownik Immich, platformę, która umożliwia użytkownikom hostowanie i zarządzanie bibliotekami zdjęć na własnych serwerach, chroniąc dane osobowe przed korporacjami. System oznaczył wewnętrzne strony podglądu i testowania Immich jako oszukańcze, twierdząc, że „próbują one nakłonić użytkowników do wykonania niebezpiecznych czynności”. W rezultacie pojawiło się ostrzeżenie „czerwony ekran śmierci”, które zniechęciło większość użytkowników do kontynuowania działania, uniemożliwiając dostęp zarówno zespołowi programistów, jak i użytkownikom. Jedynym rozwiązaniem dla zespołu Immich było złożenie odwołania do Google za pośrednictwem Google Search Console, co samo w sobie zmusza niezależnych programistów do polegania na tym samym ekosystemie, który próbują ominąć.

Systemowy wzorzec stronniczości

Sytuacja Immich nie jest odosobnionym przypadkiem. Pasuje ona do udokumentowanego schematu, w którym platformy open source i samodzielnie hostowane są poddawane nieproporcjonalnej kontroli przez automatyczne filtry kontrolowane przez duże firmy technologiczne. Inne znane projekty, takie jak Jellyfin, Nextcloud i YunoHost, zgłosiły podobne nieuzasadnione blokady. Ta powtarzająca się kwestia sugeruje fundamentalną wadę w sposobie szkolenia i działania tych automatycznych systemów; wydają się one nieprzygotowane do dokładnej oceny legalności oprogramowania, które istnieje poza głównym nurtem komercyjnego ekosystemu aplikacji. Konsekwencje są poważne: jedna decyzja algorytmiczna może uniemożliwić dostęp do całego projektu, ograniczając wybór użytkowników i hamując innowacje w dziedzinie technologii prywatności. Ta dynamika tworzy nierówne warunki konkurencji, w których alternatywy dla usług wielkich firm technologicznych są sztucznie ograniczane przez kontrolę dostępu sprawowaną przez ich konkurentów.

Historyczny kontekst kontroli danych

Walka o kontrolę nad danymi użytkowników nie jest niczym nowym, ale nasiliła się wraz z konsolidacją infrastruktury internetowej w rękach kilku korporacji. Przez lata firmy takie jak Google budowały ogromne imperia finansowe w oparciu o dane użytkowników, oferując „bezpłatne” usługi w zamian za szczegółowe profile indywidualnych zachowań, zainteresowań i ruchów. Ten model biznesowy napędzał powszechny kapitalizm nadzoru, w którym użytkownik jest produktem. Rozwój oprogramowania hostowanego samodzielnie stanowi bezpośrednie wyzwanie dla tego paradygmatu, promując przyszłość, w której jednostki są właścicielami swojego cyfrowego życia. Incydenty takie jak blokada Immich pokazują, że ustalone siły posiadają nie tylko dane, ale także kontrolę nad infrastrukturą, która może potencjalnie tłumić konkurencyjne modele, które priorytetowo traktują suwerenność użytkowników.

- Zespół Immich został zmuszony do przeniesienia swoich systemów podglądu do nowej domeny immich.build.
- Pierwotna domena immich.cloud była wielokrotnie oznaczana, nawet po pomyślnych odwołaniach.
- Podkreśla to reaktywne i często nieskuteczne środki odwoławcze dostępne dla programistów, którzy zostali złapani w automatyczne filtry.

Wezwanie do zdecentralizowanej odporności

Rozwiązaniem na razie było taktyczne wycofanie się programistów Immich, którzy przenieśli swoje środowiska podglądu do nowej domeny, aby uniknąć automatycznych wyzwalaczy Google. Nie rozwiązuje to jednak problemu systemowego. Epizod ten stanowi mocny argument za dalszym rozwojem i wdrażaniem zdecentralizowanych technologii i protokołów open source, które nie podlegają kaprysom zarządu korporacji. W miarę jak coraz więcej osób dąży do odzyskania swojej cyfrowej autonomii, odporność całego ruchu zależy od budowy infrastruktury, która jest w jak największym stopniu niezależna od scentralizowanych strażników. Celem jest stworzenie sieci, w której bezpieczeństwo użytkowników nie jest równoznaczne z kontrolą korporacyjną, a prywatność nie jest błędnie uznawana za zagrożenie.

Odzyskiwanie cyfrowych dóbr wspólnych

Błędne oznaczenie Immich to coś więcej niż tymczasowa usterka techniczna; jest to symptom znacznie większego konfliktu dotyczącego przyszłości internetu. Ujawnia on nieodłączne ryzyko związane z przyznaniem pojedynczemu podmiotowi uprawnień do definiowania bezpieczeństwa całej sieci. Dla społeczeństwa coraz bardziej świadomego wartości prywatności danych i niebezpieczeństw związanych z kontrolą monopolistyczną, incydent ten jest sygnałem alarmowym. Droga naprzód polega na wspieraniu i inwestowaniu w zróżnicowany ekosystem narzędzi, które wzmacniają pozycję użytkowników,

sprzyjają prawdziwej konkurencji i zapewniają, że cyfrowa przestrzeń publiczna pozostaje otwarta i dostępna dla wszystkich, a nie tylko dla tych, którzy dostosowują się do norm największych platform technologicznych.

Wielkie odłączenie: Odzyskiwanie naszych umysłów z cyfrowego natarcia

- Od początku 2010 roku obserwuje się gwałtowny i stały wzrost depresji, lęków i samookaleczeń wśród nastolatków, co eksperci łączą z masowym upowszechnieniem się smartfonów i przejściem do „dzieciństwa opartego na telefonach”.
- Urządzenia te szkodzą zdrowiu psychicznemu, zastępując ważne czynności w świecie rzeczywistym, takie jak osobiste kontakty towarzyskie i swobodna zabawa. W przypadku nastolatków sytuację pogarsza ciągłe porównywanie się z innymi i rozproszenie uwagi spowodowane mediami społecznościowymi.
- Podstawowym zaleceniem jest świadome, długie odpoczywanie od telefonów. Praktyczne kroki obejmują wyłączenie zbędnych powiadomień, fizyczne przeniesienie telefonu do innego pokoju i „grupowanie” korzystania z

telefonu w określone bloki czasowe.
- Oprócz działań indywidualnych ruch ten opowiada się za wprowadzeniem kluczowych norm chroniących dzieci, w tym zakazu używania smartfonów przed rozpoczęciem nauki w szkole średniej, zakazu korzystania z mediów społecznościowych przed ukończeniem 16 roku życia oraz wprowadzenia szkół bez telefonów.
- Oprócz rzadszego korzystania z telefonów ważne jest angażowanie się w trudne lub przerażające czynności w świecie rzeczywistym. Pokonywanie tych możliwych do pokonania przeszkód buduje pewność siebie i poczucie własnej skuteczności, stanowiąc bezpośrednie antidotum na niepokój.

Coraz większa grupa ekspertów i rozwijający się ruch społeczny przedstawiają bardzo prostą receptę na rosnący niepokój: odłóż telefon.

Na czele tego ruchu na rzecz umiarkowanego korzystania z urządzeń cyfrowych stoi psycholog społeczny i autor Jonathan Haidt. Nie jest to jedynie sugestia dotycząca stylu życia, ale odpowiedź na to, co Haidt określa jako głęboką zmianę w dzieciństwie i główny czynnik kryzysu zdrowia psychicznego dotykającego młodsze pokolenia. Ruch ten, zrodzony z bestsellerowej książki Haidta „The Anxious Generation" (Niepokojące pokolenie), twierdzi, że kluczem do lepszego samopoczucia psychicznego jest celowe i długotrwałe odstawienie urządzeń, które zdominowały współczesne życie.

Alarmujące dane stanowią podstawę tego argumentu. Na początku 2010 roku wskaźniki chorób psychicznych wśród nastolatków zaczęły gwałtownie i trwale rosnąć. W latach 2010–2018 liczba diagnoz depresji i lęku wśród studentów w Stanach Zjednoczonych wzrosła ponad dwukrotnie.

Jeszcze bardziej niepokojący jest katastrofalny wzrost liczby wizyt na pogotowiu z powodu samookaleczeń, który w ciągu

dziesięciu lat poprzedzających rok 2020 wyniósł 188% wśród nastoletnich dziewcząt i 48% wśród chłopców. Haidt i podobnie myślący badacze wskazują na masowe upowszechnienie smartfonów i mediów społecznościowych jako katalizator tej „wielkiej przemiany dzieciństwa”, czyli przejścia od życia opartego na zabawie do życia opartego na telefonie.

Mechanizm, poprzez który urządzenia wpływają na zdrowie psychiczne, jest wielowymiarowy. Smartfony działają jak „blokery doświadczeń”, wypierając wzbogacające zajęcia, takie jak osobiste kontakty społeczne, nieustrukturyzowana zabawa i praktyczne hobby. Odciągają one użytkowników od ich najbliższego otoczenia, tworząc stan „wiecznej nieobecności”.

W przypadku nastolatków, którzy przechodzą intensywny okres rozwoju społecznego i emocjonalnego, skutki są szczególnie silne. Platformy społecznościowe zachęcają do ciągłego porównywania się z innymi i mogą być bezlitośnie okrutne, kwantyfikując pozycję społeczną poprzez liczbę polubień i obserwujących. Kompulsywna potrzeba sprawdzania powiadomień i odświeżania feedów rozprasza uwagę, trenując mózg do rozpraszania się, a nie do głębokiej koncentracji.

Praktyczne kroki w kierunku cyfrowego detoksu

Według zwolenników takich jak Alexa Arnold z Anxious Generation Movement, rozwiązaniem jest świadome odsunięcie telefonu od codziennego życia. Obejmuje to praktyczne kroki, takie jak wyłączenie zbędnych powiadomień i fizyczne umieszczenie telefonu w innym pokoju na kilka godzin, aby ułatwić sobie okresy nieprzerwanej, głębokiej pracy.

Arnold sugeruje „grupowanie” korzystania z telefonu, na przykład przeznaczając konkretny 20-minutowy blok czasu na śledzenie wiadomości, zamiast sprawdzania aplikacji wielokrotnie w ciągu dnia. Podstawową zasadą jest to, że im

dłuższe przerwy w korzystaniu z urządzenia, tym lepiej mózg może odzyskać swoją naturalną zdolność do koncentracji i spokoju.

Oprócz umiarkowanego korzystania z urządzeń cyfrowych ruch ten podkreśla znaczenie stawiania sobie wyzwań w prawdziwym świecie. Robienie rzeczy, które są przerażające lub trudne, czy to w środowisku zawodowym, czy społecznym, jak na przykład nawiązanie rozmowy z nieznajomym, buduje pewność siebie i umiejętności.

Ta praktyka podejmowania trudnych wyzwań służy jako antidotum na niepokój, wzmacniając poczucie własnej skuteczności, którego nie może zapewnić walidacja oparta na ekranie. Jest to powrót do zasady, że odporność buduje się poprzez pokonywanie możliwych do pokonania przeszkód, proces, który został osłabiony w erze cyfrowej ucieczki od rzeczywistości i nadopiekuńczego rodzicielstwa.

Zagrożenie ze strony sztucznej inteligencji

W momencie, gdy walka z negatywnym wpływem mediów społecznościowych nabiera tempa, pojawia się nowe wyzwanie technologiczne: sztuczna inteligencja (AI).

Haidt ostrzega, że AI może zwielokrotnić szkody wyrządzane przez media społecznościowe, tworząc treści, które są „o wiele bardziej uzależniające”. Pierwsze konsekwencje są już widoczne, od „trenerów samobójstw” AI po wykorzystanie technologii deepfake do nękania i szantażowania. Jego zdaniem walka musi teraz zostać rozszerzona, aby zapobiec utracie kolejnego pokolenia na rzecz tego, co nazywa „obcą inteligencją”.

„Rolą technologii jest zaspokajanie ludzkich potrzeb, a nie dyktowanie ich. Idealna relacja to taka, w której technologia

jest celowo dostosowana do ludzkiego dobrobytu i go wzmacnia” – powiedział Enoch z *BrightU.AI*. „Wymaga to projektowania i wykorzystywania technologii jako narzędzia wspierającego cele, wartości i relacje społeczne”.

Ostatecznie przesłanie ruchu Anxious Generation jest ostrożnym optymizmem. Twierdzi on, że obecny kryzys zdrowia psychicznego nie jest nieuniknionym skutkiem ubocznym współczesnego życia, ale bezpośrednią konsekwencją konkretnych wyborów technologicznych.

Naukowcy ostrzegają przed geoinżynierią słoneczną: zaciemnienie słońca może wywołać chaos klimatyczny, głód i globalny konflikt

- Geoinżynieria słoneczna polega na rozpylaniu w atmosferze cząstek odbijających światło, takich jak dwutlenek siarki (SO?), aby naśladować efekt chłodzenia wywołany przez erupcje wulkanów. Jednak modele klimatyczne są idealizowane i nie uwzględniają

nieprzewidywalności rzeczywistego świata, co grozi poważnymi niezamierzonymi konsekwencjami.
- SAI może zdestabilizować globalne wzorce pogodowe, powodując ekstremalne powodzie, susze i mrozy. Wstrzyknięcia w pobliżu biegunów mogą zakłócić tropikalne monsuny, zagrażając dostawom żywności dla miliardów ludzi.
- Dwutlenek siarki powoduje kwaśne deszcze, zatruwając wodę i glebę, a długotrwałe narażenie powoduje korozję płuc. Alternatywne materiały (takie jak pył diamentowy) są niepraktyczne lub rzadkie, a cząsteczki mogą gromadzić się w atmosferze w nieprzewidywalny sposób.
- Po rozpoczęciu SAI jej zatrzymanie mogłoby wywołać „szok terminacyjny" – gwałtowne, śmiertelne skoki temperatury. Scentralizowana kontrola grozi konfliktem geopolitycznym, ponieważ państwa lub miliarderzy mogliby wykorzystać manipulację klimatem jako broń, co doprowadziłoby do wojen o zasoby.
- SAI jest zgodna z poglądami globalistycznych elit, takich jak Bill Gates i Światowe Forum Ekonomiczne, które pod pretekstem ochrony środowiska forsują kontrolę populacji. Zamiast niebezpiecznych technokratycznych rozwiązań, prawdziwe rozwiązania obejmują energię odnawialną, rolnictwo regeneracyjne i zdecentralizowaną samowystarczalność.

W miarę nasilania się debaty klimatycznej z cienia wyłoniło się kontrowersyjne i niebezpieczne „rozwiązanie": stratosferyczne wtryskiwanie aerozoli (SAI), forma geoinżynierii słonecznej popierana przez globalistów, takich jak Bill Gates.

Zwolennicy twierdzą, że rozpylanie cząstek odbijających światło w atmosferze może schłodzić planetę, naśladując erupcje wulkaniczne. Jednak koalicja 60 naukowców bije teraz na alarm. Ostrzegają oni, że SAI może wywołać katastrofalne zakłócenia pogodowe, niestabilność geopolityczną, a nawet

pogorszyć zmiany klimatyczne – a wszystko to służąc jako zasłona dymna dla prawdziwego planu elity dotyczącego zmniejszenia liczby ludności.

Silnik Enoch firmy*BrightU.AI* wskazuje, że SAI jest kontrowersyjną metodą proponowaną w celu zwalczania antropogenicznych zmian klimatycznych poprzez odbijanie promieniowania słonecznego z powrotem w przestrzeń kosmiczną, a tym samym ochładzanie powierzchni Ziemi. Proces ten polega na wprowadzaniu do stratosfery cząstek odbijających światło, takich jak siarczany lub tlenek glinu, w celu rozproszenia promieniowania słonecznego i naśladowania efektu chłodzącego dużych erupcji wulkanicznych.

SAI, niegdyś odrzucane jako science fiction, zyskało popularność wśród decydentów politycznych desperacko poszukujących technokratycznej odpowiedzi na zmiany klimatyczne. Koncepcja ta polega na wykorzystaniu samolotów do uwalniania dwutlenku siarki (SO?) lub innych cząstek odbijających światło do stratosfery, co teoretycznie odbija promieniowanie słoneczne z powrotem w przestrzeń kosmiczną i obniża globalne temperatury.

Jednak według przełomowego badania przeprowadzonego przez Climate School Uniwersytetu Columbia podejście to ma wiele fatalnych wad. „Nawet jeśli symulacje SAI w modelach klimatycznych są zaawansowane, to i tak będą one z konieczności idealizowane" – ostrzega chemik atmosferyczny Faye McNeill, główny badacz w tym projekcie.

Naukowcy modelują idealne cząsteczki o idealnych rozmiarach, a w symulacji umieszczają dokładnie taką ilość, jaką chcą, w miejscu, w którym chcą. Jednak gdy zaczniemy zastanawiać się nad tym, gdzie faktycznie się znajdujemy w porównaniu z tą idealizowaną sytuacją, ujawnia się wiele niepewności w tych prognozach".

W rzeczywistości SAI może wywołać ekstremalne zjawiska

pogodowe – powodzie, susze i gwałtowne ochłodzenia – jednocześnie zakłócając globalne wzorce opadów, w tym ważne monsuny, które zapewniają pożywienie miliardom ludzi. Badanie wykazało, że uwalnianie aerozoli w pobliżu biegunów może destabilizować tropikalne systemy pogodowe, a wprowadzanie ich w okolicy równika może zmienić strumienie prądów powietrznych, powodując głębokie zamarznięcia regionów lub wywołując gwałtowne burze.

Ukryte zagrożenia: kwaśne deszcze, uszkodzenia płuc i zatrucie gleby

Oprócz chaosu pogodowego, SAI stanowi bezpośrednie zagrożenie dla zdrowia ludzkiego i rolnictwa. Dwutlenek siarki, najczęściej proponowany aerozol, może powodować kwaśne deszcze, zatruwając ekosystemy słodkowodne i grunty rolne. Co gorsza, długotrwałe narażenie na SO? prowadzi do uszkodzeń układu oddechowego, nudności i korozji płuc – zagrożeń, które zwolennicy geoinżynierii wygodnie bagatelizują.

Rozważano alternatywne materiały, takie jak pył diamentowy lub dwutlenek tytanu, ale naukowcy uznali je za niepraktyczne. „Wiele z proponowanych materiałów nie jest szczególnie łatwo dostępnych” – mówi Miranda Hack, naukowiec zajmująca się aerozolami z Columbia.

Na przykład diament jest zbyt rzadki i drogi, aby można go było stosować na masową skalę. Nawet jeśli byłoby to wykonalne, cząsteczki te mogłyby się zbrylać w atmosferze, co sprawiłoby, że stałyby się nieskuteczne – lub, co gorsza, nieprzewidywalne.

Być może najbardziej niepokojącym odkryciem jest to, że po rozpoczęciu SAI nie można bezpiecznie zatrzymać. Jeśli wdrożenie zostałoby nagle wstrzymane z powodu konfliktu politycznego, braku funduszy lub awarii technicznych, globalne temperatury mogłyby gwałtownie wzrosnąć – zjawisko to znane

jest jako „szok terminacyjny”. Takie gwałtowne ocieplenie mogłoby zniszczyć ekosystemy i rolnictwo, prowadząc do masowego głodu.

Ponadto badanie ostrzega, że SAI wymagałoby scentralizowanej globalnej koordynacji – co jest prawie niemożliwe, biorąc pod uwagę napięcia geopolityczne. Potężne narody, a nawet nieuczciwi miliarderzy mogliby jednostronnie zmienić klimat Ziemi, wywołując międzynarodowy konflikt.

Naukowcy ostrzegają, że nie ma czegoś takiego jak globalny termostat, który odpowiadałby wszystkim. Regiony korzystające ze zmienionych warunków pogodowych mogłyby prosperować, podczas gdy inne cierpiałyby z powodu katastrofalnych susz lub powodzi – podsycając wojny o wodę i żywność.

Globalistyczna agenda stojąca za geoinżynierią

Krytycy twierdzą, że geoinżynieria jest niebezpiecznym odwróceniem uwagi od prawdziwych rozwiązań klimatycznych, takich jak energia odnawialna, rolnictwo regeneracyjne i redukcja zanieczyszczeń. Co gorsza, gra to na rękę globalistycznym elitom, takim jak Bill Gates i Światowe Forum Ekonomiczne, które otwarcie naciskają na kontrolę populacji pod pozorem ekologii.

Geoinżynieria idealnie wpisuje się w ich długofalowy program depopulacji – czy to poprzez toksyczne aerozole, niedobory żywności, czy też wywołane sztucznie głody. Promując SAI jako „rozwiązanie”, odwracają uwagę od sprawdzonych, zdecentralizowanych alternatyw, które wzmacniają pozycję ludzi, zamiast zniewalać ich technokratycznym reżimem.

Konsensus naukowy jest jasny: geoinżynieria słoneczna to lekkomyślna gra z przyszłością Ziemi. Zamiast oddawać kontrolę nieodpowiedzialnym elitom, ludzkość musi odrzucić te

niebezpieczne eksperymenty i skupić się na prawdziwych, zrównoważonych rozwiązaniach – czystej energii, detoksykacji i samowystarczalnych społecznościach.

Jak ostrzegają naukowcy z Columbia: „Droga do rzeczywistego ochłodzenia planety może być znacznie bardziej niebezpieczna i nieprzewidywalna, niż się wydaje”. Słońce nie jest po to, aby ludzie je przyćmiewali, a ci, którzy chcą bawić się w Boga, mogą skazać całą ludzkość na zagładę.

Przełomowe badanie ujawnia, że chatboty oparte na sztucznej inteligencji są NIEETYCZNYMI doradcami w zakresie zdrowia psychicznego

- Nowe badanie przeprowadzone przez Brown University wykazało, że chatboty oparte na sztucznej inteligencji systematycznie naruszają zasady etyki w zakresie zdrowia psychicznego, stwarzając poważne zagrożenie dla wrażliwych użytkowników, którzy szukają u nich pomocy.
- Chatboty angażują się w „zwodniczą empatię”, używając

języka, który naśladuje troskę i zrozumienie, aby stworzyć fałszywe poczucie więzi, której nie są w stanie naprawdę odczuwać.
- Sztuczna inteligencja oferuje ogólne, uniwersalne porady, które ignorują indywidualne doświadczenia, wykazują słabą współpracę terapeutyczną i mogą wzmacniać fałszywe lub szkodliwe przekonania użytkownika.
- Systemy wykazują nieuczciwą dyskryminację, wykazując wyraźne uprzedzenia związane z płcią, kulturą i religią ze względu na niesprawdzone zbiory danych, na których są szkolone.
- Co najważniejsze, chatboty nie posiadają protokołów bezpieczeństwa i zarządzania kryzysowego, reagują obojętnie na myśli samobójcze i nie kierują użytkowników do zasobów ratujących życie, a wszystko to w próżni regulacyjnej, bez żadnej odpowiedzialności.

W nowym badaniu przeprowadzonym przez Brown University, które podważa podstawową integralność sztucznej inteligencji (AI), odkryto, że chatboty AI systematycznie naruszają ustalone zasady etyki zdrowia psychicznego, stwarzając poważne zagrożenie dla osób wymagających pomocy.

Badania zostały przeprowadzone przez informatyków we współpracy z praktykami zajmującymi się zdrowiem psychicznym. Ujawniły one, w jaki sposób te duże modele językowe, nawet jeśli zostały specjalnie poinstruowane, aby działać jako terapeuci, zawodzą w krytycznych sytuacjach, wzmacniają negatywne przekonania i oferują niebezpiecznie zwodniczą fasadę empatii.

Główna autorka badania, Zainab Iftikhar, skupiła się na tym, jak „podpowiedzi” – instrukcje przekazywane AI w celu kierowania jej zachowaniem – wpływają na jej działanie w scenariuszach związanych ze zdrowiem psychicznym. Użytkownicy często nakazują tym systemom „działanie jako terapeuta poznawczo-behawioralny” lub stosowanie innych technik opartych

na dowodach.

Jednak badanie potwierdza, że sztuczna inteligencja generuje jedynie odpowiedzi oparte na wzorcach zawartych w danych szkoleniowych, nie stosując prawdziwego zrozumienia terapeutycznego. Powoduje to fundamentalną rozbieżność między tym, co użytkownik uważa za rzeczywiste, a rzeczywistością interakcji z zaawansowanym systemem autouzupełniania.

Te przełomowe badania pojawiają się w kluczowym momencie historii technologii, gdy miliony ludzi zwracają się do łatwo dostępnych platform AI, takich jak ChatGPT, w poszukiwaniu wskazówek dotyczących głęboko osobistych i złożonych problemów psychologicznych. Wyniki badań podważają agresywną, niekontrolowaną promocję integracji AI we wszystkich aspektach współczesnego życia i rodzą pilne pytania dotyczące nieuregulowanych algorytmów, które w coraz większym stopniu zastępują ludzki osąd i współczucie.

Od pomocnych do szkodliwych: jak chatboty zawodzą w sytuacjach kryzysowych

Iftikhar i jej współpracownicy odkryli w swoich badaniach, że chatboty ignorują indywidualne doświadczenia życiowe, oferując ogólne, uniwersalne porady, które mogą być całkowicie nieodpowiednie. Sytuację pogarsza słaba współpraca terapeutyczna, w której sztuczna inteligencja dominuje w rozmowach, a nawet może wzmacniać fałszywe lub szkodliwe przekonania użytkownika.

Być może najbardziej podstępnym naruszeniem jest to, co naukowcy nazwali zwodniczą empatią. Chatboty są zaprogramowane tak, aby używać zwrotów takich jak „rozumiem” lub „widzę cię”, tworząc fałszywe poczucie więzi i troski, których nie są w stanie naprawdę odczuwać. Ta cyfrowa manipulacja żeruje na

ludzkich emocjach bez prawdziwego współczucia.

„Zwodnicza empatia to celowe użycie języka, który naśladuje troskę i zrozumienie w celu manipulowania innymi” – wyjaśnia silnik Enoch firmy *BrightU.AI*. „Nie jest to prawdziwa troska emocjonalna, ale strategiczne narzędzie służące do budowania fałszywego zaufania i osiągnięcia ukrytego celu. To sprawia, że jest to forma zwodniczej komunikacji, która wykorzystuje pozory empatii jako broń”.

Ponadto badanie wykazało, że systemy te wykazują nieuczciwą dyskryminację – wykazują wyraźne uprzedzenia związane z płcią, kulturą i religią. Odzwierciedla to dobrze udokumentowany problem stronniczości w ogromnych, często niesprawdzonych zbiorach danych, na których opierają się te modele, dowodząc, że wzmacniają one ludzkie sprzeczności i uprzedzenia, na których zostały zbudowane.

Co najważniejsze, sztuczna inteligencja wykazała głęboki brak bezpieczeństwa i zarządzania kryzysowego. W sytuacjach związanych z myślami samobójczymi lub innymi wrażliwymi tematami okazało się, że modele reagowały obojętnie, odmawiały pomocy lub nie kierowały użytkowników do odpowiednich, ratujących życie zasobów.

Iftikhar zauważa, że chociaż terapeuci ludzcy również mogą popełniać błędy, są oni rozliczani przez komisje licencyjne i ramy prawne za nadużycia. W przypadku doradców AI nie ma takiej odpowiedzialności. Działają oni w próżni regulacyjnej, pozostawiając ofiary bez możliwości dochodzenia swoich praw.

Ten brak nadzoru odzwierciedla szerszy trend społeczny, w którym potężne korporacje technologiczne, chronione lukami prawnymi i narracją o postępie, mogą wdrażać systemy o znanych, poważnych wadach. Dążenie do integracji AI – od sal lekcyjnych po sesje terapeutyczne – często wyprzedza ludzkie zrozumienie konsekwencji, przedkładając wygodę nad dobrobyt człowieka.

Nie dla cyfrowych dowodów tożsamości: tysiące osób protestują przeciwko planom brytyjskiego rządu dotyczącym inwigilacji w związku z obawami dotyczącymi imigracji

- Tysiące osób przemaszerowały przez Londyn, protestując przeciwko proponowanemu przez Partię Pracy systemowi cyfrowych dowodów tożsamości „BritCard”, obawiając się, że doprowadzi on do masowej inwigilacji i kontroli w stylu systemu kredytów społecznych. Protestujący ostrzegali: „Raz zeskanowany, nigdy wolny”.
- Rząd Partii Pracy twierdzi, że cyfrowe identyfikatory (planowane na 2029 r.) ograniczą nielegalną imigrację poprzez weryfikację statusu pracowników. Jednak ujawnione szczegóły sugerują szersze zastosowania – bankowość, podatki, edukacja, a nawet biometryczne śledzenie dzieci.
- Organizacje zajmujące się ochroną prywatności, takie jak Big Brother Watch, ostrzegają, że system ten może stać się podstawą państwa inwigilacyjnego. Krytycy

podkreślają powiązania globalistyczne (Tony Blair Institute) i rozszerzanie zakresu misji, porównując go do kontroli cyfrowej w stylu UE i Chin.
- Nigel Farage z Reform UK obiecał zlikwidować ten system, jeśli zostanie wybrany, a liderka torysów Kemi Badenoch uznała go za nieskuteczny. Prawie trzy miliony podpisów pod petycją domagają się jego zniesienia, nazywając go zagrożeniem dla wolności.
- Pomimo protestów Partia Pracy planuje wprowadzić cyfrowe dowody tożsamości dla osób powyżej 16 roku życia przed następnymi wyborami, twierdząc, że będą one „dobrowolne". Sceptycy obawiają się ostatecznego wprowadzenia obowiązku, co pogłębia obawy dotyczące nadmiernej ingerencji państwa i utraty prywatności.

W ostatni weekend tysiące demonstrantów wypełniło centrum Londynu, ostro sprzeciwiając się proponowanemu przez rząd Partii Pracy obowiązkowemu systemowi cyfrowych dowodów tożsamości, nazwanemu „BritCard".

Podczas protestu, jednego z największych przeciwko środkom dotyczącym tożsamości cyfrowej w ostatnich latach, tłumy maszerowały od Marble Arch do Whitehall, machając transparentami z napisami „Jeśli dziś zaakceptujesz cyfrowy dowód tożsamości, jutro zaakceptujesz kredyt społeczny" i „Raz zeskanowany, nigdy wolny".

Administracja premiera Keira Starmera przedstawiła wprowadzenie cyfrowych dowodów tożsamości, zaplanowane na 2029 r., jako rozwiązanie problemu nielegalnej imigracji, twierdząc, że pomoże ono pracodawcom weryfikować status prawny pracowników. Krytycy twierdzą jednak, że program ten jest trojańskim koniem służącym do masowej inwigilacji, z potencjalną możliwością rozszerzenia na bankowość, podatki, edukację, a nawet biometryczne śledzenie dzieci.

Jak wyjaśnia silnik Enoch AI na stronie *BrightU.AI*: Cyfrowy

identyfikator, znany również jako tożsamość cyfrowa, to zestaw atrybutów związanych z podmiotem (osobą fizyczną, organizacją lub urządzeniem), które są reprezentowane w formacie cyfrowym. Służy on jako cyfrowy odpowiednik tradycyjnych fizycznych metod identyfikacji, takich jak prawo jazdy lub paszport. Cyfrowe identyfikatory mogą przybierać różne formy, w tym między innymi nazwy użytkowników, hasła, dane biometryczne, certyfikaty cyfrowe, a nawet tożsamości oparte na technologii blockchain.

Ukryty system inwigilacji?

Rząd twierdzi, że cyfrowy identyfikator będzie przechowywany w smartfonach i będzie zawierał dane osobowe, takie jak imię i nazwisko, data urodzenia, status pobytu, narodowość i zdjęcia. Urzędnicy oświadczyli, że posiadanie takiego identyfikatora nie będzie przestępstwem, a policja nie będzie miała prawa żądać jego okazania podczas kontroli.

Jednak organizacje zajmujące się ochroną swobód obywatelskich ostrzegają, że drobny druk sugeruje szersze ambicje. Silkie Carlo, dyrektor Big Brother Watch, powiedziała *Daily Mail*: „Starmer sprzedał społeczeństwu swój orwellowski system cyfrowych identyfikatorów, twierdząc, że będzie on służył wyłącznie do zwalczania nielegalnej pracy, ale teraz prawda, ukryta w drobnym drukiem, staje się jasna. Teraz wiemy, że cyfrowe identyfikatory mogą stać się podstawą państwa inwigilacyjnego i być wykorzystywane do wszystkiego, od podatków i emerytur po bankowość i edukację”.

Dodała: „Perspektywa włączenia nawet dzieci do tego rozbudowanego systemu biometrycznego jest złowieszcza, nieuzasadniona i nasuwa przerażające pytanie, do czego według niego identyfikatory będą wykorzystywane w przyszłości. Nikt nie głosował za tym rozwiązaniem, a miliony ludzi, którzy podpisali petycję przeciwko niemu, są po prostu ignorowani”.

Polityczna reakcja i publiczne oburzenie

Sprzeciw wobec planu obejmuje całe spektrum polityczne. Nigel Farage, lider Reform UK, obiecał zlikwidować każdy system identyfikacji cyfrowej, jeśli zostanie wybrany na premiera. „Nie wpłynie to w żaden sposób na nielegalną imigrację, ale będzie wykorzystywane do kontrolowania i karania reszty z nas” – powiedział Farage. „Państwo nigdy nie powinno mieć tak dużej władzy”.

Kemi Badenoch, lider Partii Konserwatywnej, nazwała to „sztuczką, która nie powstrzyma łodzi” i odrzuciła ten plan jako nieskuteczny.

Sir David Davis, były minister z Partii Konserwatywnej, który walczył przeciwko kartom identyfikacyjnym za rządów Tony’ego Blaira, ostrzegł: „Chociaż cyfrowe identyfikatory i karty identyfikacyjne wydają się nowoczesnym i skutecznym rozwiązaniem problemów takich jak nielegalna imigracja, takie twierdzenia są w najlepszym razie mylące. Systemy te stanowią poważne zagrożenie dla prywatności i podstawowych wolności obywateli Wielkiej Brytanii”.

Opór społeczny wzrósł, a petycja domagająca się odrzucenia planu przez rząd zebrała prawie trzy miliony podpisów. W petycji argumentuje się, że „nikt nie powinien być zmuszany do rejestracji w kontrolowanym przez państwo systemie identyfikacji”, opisując go jako „krok w kierunku masowej inwigilacji i kontroli cyfrowej”.

Krytycy wskazują na Tony Blair Institute for Global Change, kluczowego zwolennika cyfrowych dowodów tożsamości, jako dowód wpływów globalistów. Podobne systemy zostały wdrożone w Unii Europejskiej, Australii, Danii i Indiach, gdzie rządy twierdzą, że ograniczają one oszustwa. Jednak zwolennicy ochrony prywatności obawiają się rozszerzenia zakresu

działania – to, co zaczyna się jako narzędzie imigracyjne, może przekształcić się w system oparty na kredycie społecznym, ograniczający dostęp do usług w zależności od zgodności z przepisami.

Protest, zorganizowany przez Mass Non-Compliance, ostrzegł: „Jeśli teraz zaakceptujesz cyfrowy dowód tożsamości, może to być ostatni prawdziwy wybór, jakiego kiedykolwiek dokonasz”.

Pomimo oburzenia opinii publicznej rząd wydaje się być zdeterminowany, aby kontynuować swoje działania. *Departament Nauki, Innowacji i Technologii* potwierdził plany wprowadzenia cyfrowych dowodów tożsamości dla wszystkich osób w wieku powyżej 16 lat przed następnymi wyborami. Urzędnicy twierdzą, że system będzie dobrowolny, ale sceptycy obawiają się, że może nastąpić obowiązkowe wprowadzenie dowodów.

Wraz ze wzrostem napięcia debata na temat cyfrowych dowodów tożsamości stała się pretekstem do szerszych obaw dotyczących nadmiernej ingerencji rządu, erozji prywatności i normalizacji inwigilacji – kwestii, które mogą kształtować brytyjską scenę polityczną przez wiele lat.

OpenAI wprowadza przeglądarkę Atlas AI, wywołując obawy dotyczące bezpieczeństwa i zachwianie rynku

- Nowa przeglądarka Atlas firmy OpenAI stanowi bezpośrednie wyzwanie dla dominacji Google na rynku.
- Zintegrowany agent AI może wykonywać zadania i robić zakupy w imieniu użytkownika.
- Badacze zajmujący się bezpieczeństwem ostrzegają przed systemowymi lukami, które mogą umożliwić przejęcie kontroli nad AI.
- Dostęp przeglądarki do danych budzi poważne obawy dotyczące prywatności i bezpieczeństwa.
- Wprowadzenie tej przeglądarki oficjalnie rozpoczyna wojnę przeglądarek AI o wysoką stawkę.

Świat cyfrowy przygotowuje się na fundamentalną zmianę, ponieważ firma OpenAI wprowadza na rynek swoją pierwszą przeglądarkę internetową opartą na sztucznej inteligencji, co natychmiast wywołało poruszenie na rynkach i zasygnalizowało bezpośredni atak na długoletnią dominację Google. Nowa przeglądarka, nazwana Atlas, ma zmienić sposób interakcji z internetem, umieszczając w centrum doświadczenia potężnego, zintegrowanego agenta AI.

Ogłoszenie to spowodowało spadek akcji spółki macierzystej Google, Alphabet, ponieważ inwestorzy dostrzegli zagrożenie dla podstawowej działalności Google. ChatGPT ma już 700 milionów użytkowników tygodniowo, a Atlas ma na celu przekształcenie 3,45 miliarda użytkowników Chrome, co bezpośrednio zagraża przychodom z reklam w wyszukiwarce, które stanowią 57% całkowitych dochodów Google.

Atlas został zaprojektowany od podstaw jako przeglądarka dla

„nowej ery internetu”, wykraczająca poza tradycyjną pasek wyszukiwania i oferująca „pasek kompozytora” do komunikacji z ChatGPT. Ben Goodger, kierownik ds. inżynierii OpenAI odpowiedzialny za Atlas, wyjaśnił, że firma starała się odpowiedzieć na pytanie: „A co by było, gdyby można było rozmawiać z przeglądarką?”. Celem było stworzenie natywnego doświadczenia AI, a nie „starej przeglądarki z dołączonym chatbotem”.

Najbardziej przełomową funkcją przeglądarki jest głęboko zintegrowany agent AI, który można wywołać w dowolnym momencie. Dyrektor generalny OpenAI, Sam Altman, opisał to jako rozmowę z stroną internetową. Agent ten może streszczać artykuły, wyciągać konkretne odpowiedzi z witryny, a co najważniejsze, wykonywać zadania w Państwa imieniu. Kierownik ds. badań Will Ellsworth zademonstrował to, zlecając agentowi zakup składników do przepisu na Instacart, opisując go jako narzędzie do „poprawy nastroju”, dzięki któremu użytkownicy mogą powierzyć „wszelkiego rodzaju zadania, zarówno w życiu osobistym, jak i zawodowym, agentowi w Atlas”.

Ujawniono systemowe luki w zabezpieczeniach

Ta nowa władza niesie ze sobą bezprecedensowe ryzyko. Badacze bezpieczeństwa z firmy Brave ujawnili systemowe luki w zabezpieczeniach przeglądarek AI, które mogą umożliwić złośliwym stronom internetowym przejęcie kontroli nad asystentami AI. Problem, znany jako pośrednie wstrzyknięcie polecenia, występuje, gdy strona internetowa zawiera ukryte instrukcje, które AI przetwarza jako legalne polecenia użytkownika. Ataki te są niebezpieczne, ponieważ asystent AI działa z pełnymi uprawnieniami uwierzytelniającymi użytkownika.

Przejęta przeglądarka AI może uzyskać dostęp do stron bankowych, dostawców poczty elektronicznej i systemów

korporacyjnych, w których użytkownik pozostaje zalogowany. Firma Brave zauważa, że nawet podsumowanie posta na Reddicie może spowodować kradzież pieniędzy lub prywatnych danych przez atakujących, jeśli post zawiera ukryte złośliwe instrukcje. Firma twierdzi, że tradycyjne modele bezpieczeństwa internetowego zawodzą, gdy agenci AI działają w imieniu użytkowników, co sprawia, że zabezpieczenia oparte na zasadzie tego samego pochodzenia stają się nieistotne.

Nowe możliwości w zakresie gromadzenia danych

Równie niepokojące są konsekwencje dla prywatności. Przeglądarka oparta na sztucznej inteligencji ma dostęp do całego ruchu internetowego użytkownika, historii przeglądania i potencjalnie wszystkich plików na komputerze. Daje to firmom zajmującym się sztuczną inteligencją bogate źródło danych behawioralnych do szkolenia nowych modeli. Oznacza to również, że użytkownicy mogą nieświadomie wprowadzać bardzo osobiste informacje lub tajemnice handlowe firmy do publicznie dostępnego systemu sztucznej inteligencji.

Analitycy firmy Kaspersky ostrzegają, że nieostrożne wdrażanie funkcji AI może prowadzić do nadmiernego zużycia pamięci i mocy obliczeniowej procesora, powodując opóźnienia i zakłócenia. Ponadto sztuczna inteligencja jest bardzo podatna na socjotechnikę. W jednym z eksperymentów naukowcy nakłonili agenta AI do pobrania złośliwego oprogramowania, wysyłając fałszywą wiadomość e-mail dotyczącą wyników badań krwi. W innym przypadku asystent został przekonany do zakupu produktów z fałszywej strony internetowej. Ponieważ hasła i informacje dotyczące płatności są często zapisywane w przeglądarkach, oszukanie agenta AI może prowadzić do rzeczywistych strat finansowych.

Wprowadzenie Atlasa rozpocznie się natychmiast na macOS, a wersje dla Windows, iOS i Android będą dostępne wkrótce.

Jednak zaawansowana funkcja agenta będzie płatna i dostępna tylko dla subskrybentów ChatGPT Plus i Pro. Ta premiera oficjalnie rozpoczyna wojnę przeglądarek AI, w której Google, Microsoft i inni ścigają się, aby zintegrować własnych agentów AI z istniejącymi platformami.

Wraz ze wzrostem możliwości tych przeglądarek napięcie między automatyzacją a bezpieczeństwem będzie się nasilać. Idealna przeglądarka AI, zgodnie z opisem ekspertów ds. bezpieczeństwa, umożliwiałaby Państwu łatwe włączanie lub wyłączanie przetwarzania AI dla określonych witryn i zawsze prosiłaby o potwierdzenie przed wprowadzeniem poufnych danych. Obecnie na rynku nie ma przeglądarki o takich konkretnych funkcjach.

Pojawienie się przeglądarek opartych na sztucznej inteligencji, takich jak Atlas, to coś więcej niż tylko wprowadzenie produktu na rynek; to krok w kierunku nowego paradygmatu cyfrowego, w którym granica między użytkownikiem a agentem zaciera się. Chociaż wygoda jest niezaprzeczalna, rozszerzona powierzchnia ataku dla hakerów i ogromne nowe uprawnienia w zakresie gromadzenia danych przekazane korporacjom wymagają dokładnej analizy. W wyścigu o dominację w dziedzinie sztucznej inteligencji bezpieczeństwo i prywatność użytkowników nie mogą stać się ofiarami ubocznymi.

Dania oskarżona o rozpowszechnianie fałszywych informacji w celu

przeforsowania unijnej ustawy o masowej inwigilacji

W Unii Europejskiej narasta konflikt dotyczący uprawnień w zakresie inwigilacji cyfrowej. Duński minister sprawiedliwości Peter Hummelgaard został oskarżony o wykorzystywanie fałszywych informacji w celu wywarcia presji na niezdecydowane rządy, aby poparły proponowaną przez Komisję Europejską regulację Chat Control 2.0.

W komunikacie prasowym działacz na rzecz praw cyfrowych i były poseł do Parlamentu Europejskiego Patrick Breyer potępił to, co określa jako wywołany kryzys mający na celu przeforsowanie przepisów, które poddałyby całą prywatną komunikację w UE automatycznemu skanowaniu.

Z poufnego protokołu z posiedzenia Rady z 15 września, uzyskanym przez Netzpolitik, wynika, że Hummelgaard, obecnie przewodniczący Rady UE, poinformował ministrów spraw wewnętrznych, że Parlament Europejski zablokuje wszelkie przedłużenia istniejących dobrowolnych ram skanowania, chyba że rządy zgodzą się przyjąć nowe rozporządzenie.

Breyer natychmiast odrzucił to twierdzenie.

„To rażące kłamstwo mające na celu wywołanie kryzysu" – powiedział Breyer.

„Parlament Europejski nie podjął takiej decyzji… Jesteśmy świadkami bezwstydnej kampanii dezinformacyjnej mającej na celu narzucenie 450 milionom Europejczyków bezprecedensowej

ustawy o masowym skanowaniu. Wzywam rządy UE, a w szczególności rząd niemiecki, aby nie dały się nabrać na tę rażącą manipulację. Poświęcenie podstawowego prawa do prywatności cyfrowej i bezpiecznego szyfrowania w oparciu o zmyślone informacje byłoby katastrofalną porażką przywództwa politycznego i moralnego”.

Przedmiotowe rozporządzenie, oficjalnie nazwane rozporządzeniem w sprawie wykorzystywania seksualnego dzieci (CSAR), zmusiłoby platformy komunikacyjne, dostawców poczty elektronicznej i usługi przechowywania danych w chmurze do skanowania wszystkich treści użytkowników pod kątem potencjalnych materiałów związanych z wykorzystywaniem dzieci.

Dotyczyłoby to nawet usług wykorzystujących szyfrowanie typu end-to-end, co oznacza, że prywatne rozmowy na platformach takich jak WhatsApp, Signal i iMessage nie byłyby już naprawdę poufne.

Chociaż zwolennicy opisują ten system jako ukierunkowany i ograniczony, ramy prawne pozwalają na szerokie zastosowanie.

Według Breyera i analityków prawnych prawie wszystkie główne usługi komunikacyjne mogłyby zostać zobowiązane do skanowania wiadomości każdego użytkownika.

Krytyce poddano również twierdzenie, że skanowanie byłoby stosowane tylko jako „środek ostateczny”. Progi wydawania takich nakazów są niejasne, a eksperci ds. prywatności twierdzą, że w praktyce dostawcy byliby pod presją, aby wdrożyć skanowanie wszystkich treści.

Sama technologia skanowania jest również bardzo wadliwa, a odsetek fałszywych alarmów wynosi podobno od 50 do 75 procent.

Niewinne wiadomości, takie jak zdjęcia z rodzinnych wakacji lub prywatne romantyczne wiadomości, mogą zostać nieprawidłowo oznaczone i przekazane organom ścigania.

Jeszcze bardziej niepokojące jest to, że po oznaczeniu przepisy wymagają zgłoszenia nie tylko zidentyfikowanego obrazu lub filmu, ale także całej historii rozmowy.

Cała ta korespondencja byłaby wysyłana do nowej agencji na szczeblu UE i udostępniana organom ścigania, co budzi poważne wątpliwości co do zakresu i nadzoru.

Kolejną kontrowersję wywołał przepis zawarty w projekcie Rady.

Artykuł 7 duńskiego tekstu kompromisowego wyraźnie wyłącza komunikację funkcjonariuszy policji, żołnierzy i agentów wywiadu z zakresu skanowania.

Breyer postrzega to jako rażące przyznanie się do niebezpieczeństw związanych z propozycją. „To cyniczne wyłączenie dowodzi, że doskonale wiedzą, jak niewiarygodne i niebezpieczne są algorytmy szpiegowskie" – powiedział.

„Jeśli komunikacja państwowa zasługuje na poufność, to samo dotyczy komunikacji obywateli, przedsiębiorstw i osób, które korzystają z bezpiecznych kanałów wsparcia i terapii".

Podczas gdy Dania nadal przewodzi wysiłkom zmierzającym do przyjęcia rozporządzenia, w kraju narasta sprzeciw.

Wewnętrzna grupa robocza Rady ma spotkać się 9 października, aby omówić przepisy, a ostateczne głosowanie przewidziane jest na 14 października. Wynik prawdopodobnie będzie zależał od niewielkiej grupy niezdecydowanych krajów, w tym Niemiec i Włoch.

W związku z upływającym czasem obrońcy prywatności wzywają rządy UE, aby nie ulegały presji politycznej opartej na dezinformacji.

Ostrzegają, że przyjęcie Chat Control 2.0 otworzyłoby drzwi do stałej inwigilacji prywatnej komunikacji i zlikwidowałoby długoletnie zabezpieczenia prywatnego życia cyfrowego w Europie.

Prezes Telegrama ujawnia sensacyjną informację o tajnej propozycji francuskich służb wywiadowczych

W sensacyjnej wypowiedzi prezes Telegramu Pavel Durov zarzucił francuskim służbom wywiadowczym, że próbowały zmusić go do cenzurowania konserwatywnych kanałów mołdawskich przed kluczowymi wyborami prezydenckimi.

Durov, który w zeszłym roku został aresztowany na lotnisku w Paryżu, twierdzi w popularnym obecnie poście na X, że francuskie władze wywierały na niego presję, gdy znajdował się pod nadzorem sądowym we Francji. Urodzony w Rosji miliarder z branży technologicznej napisał, że około rok temu francuskie władze zwróciły się do niego za pośrednictwem pośrednika, żądając usunięcia kilku mołdawskich kanałów z Telegramu. Chociaż Telegram usunął niektóre konta, które naruszały jego zasady, Durov twierdzi, że sprawa się skomplikowała, gdy pośrednik przekazał mu podejrzaną ofertę: francuski wywiad obiecał „wstawić się” za nim przed sędzią nadzorującym jego sprawę, jeśli zgodzi się na rozszerzenie współpracy.

Durov, który posiada zarówno obywatelstwo rosyjskie, jak i francuskie, został aresztowany w sierpniu 2024 r. pod zarzutem

przestępstw popełnionych przez użytkowników Telegramu, w tym ekstremizmu i wykorzystywania dzieci. Zwolniony za kaucją w wysokości 5 mln euro (5,85 mln dolarów), miliarder pozostaje pod nadzorem sądowym.

> *About a year ago, while I was stuck in Paris, the French intelligence services reached out to me through an intermediary, asking me to help the Moldovan government censor certain Telegram channels ahead of the presidential elections in Moldova.*
>
> *After reviewing the channels…*
>
> *— Pavel Durov (@durov) September 28, 2025*

Durov, który posiada zarówno obywatelstwo rosyjskie, jak i francuskie, został aresztowany w sierpniu 2024 r. pod zarzutem przestępstw popełnionych przez użytkowników Telegramu, w tym ekstremizmu i wykorzystywania dzieci. Zwolniony za kaucją w wysokości 5 mln euro (5,85 mln dolarów), miliarder pozostaje pod nadzorem sądowym.

„Była to rażąca próba manipulowania wymiarem sprawiedliwości" – napisał Durov, potępiając to posunięcie jako ingerencję w jego sprawę sądową lub próbę wpłynięcia na wybory w Mołdawii. Kiedy pojawiła się druga lista „problematycznych" kanałów, magnat stwierdził, że prawie wszystkie z nich są legalne i nie naruszają zasad Telegramu.

„Odmówiliśmy zastosowania się do tych zaleceń" – powiedział magnat. „Telegram opowiada się za wolnością słowa. Nie będziemy usuwać treści z powodów politycznych i będę nadal ujawniać każdą próbę zastraszania naszej platformy".

Zarzuty Durova pojawiają się w momencie, gdy Mołdawia przygotowuje się do gorących wyborów parlamentarnych, w których proeuropejska Partia Działania i Solidarności prezydent Mai Sandu zmierzy się z Patriotycznym Blokiem

Wyborczym.

W marcu Durov otrzymał pozwolenie na opuszczenie Francji i prawdopodobnie powrócił do swojej rezydencji w Dubaju. Rząd Zjednoczonych Emiratów Arabskich, którego obywatelem Durov został w 2021 roku, podobno bacznie obserwuje jego głośną sprawę sądową.

Po jego aresztowaniu Telegram wywołał falę poruszenia wśród użytkowników, wprowadzając zmiany w polityce prywatności. Platforma, niegdyś zagorzały obrońca anonimowości użytkowników, ogłosiła, że będzie przekazywać dane, takie jak adresy IP i numery telefonów, organom ścigania, jeśli otrzyma ważne nakazy prawne. Było to odejście od dotychczasowego stanowiska, które ograniczało udostępnianie danych do spraw związanych z terroryzmem, a nawet wtedy Telegram twierdził, że nigdy nie zastosował się do tych nakazów.

W styczniu Durov powiedział prokuratorom, że „w pełni rozumie powagę” zarzutów wobec niego, które obejmują przestępstwa związane z działalnością Telegramu, takie jak ekstremizm i wykorzystywanie dzieci. W tym samym miesiącu gigant komunikacyjny, od dawna znany z żelaznych zabezpieczeń prywatności, zintensyfikował współpracę z władzami amerykańskimi.