NOWE KODY TOŻSAMOŚCI - CZY POWINNIŚMY STAWIAĆ GRANICE ROZWOJOWI BIOMETRII

WPROWADZENIE

Od niedawna Polacy mają możliwość stworzenia cyfrowego dowodu tożsamości poprzez skanowanie tęczówki oka. Wystarczy wziąć udział w projekcie Worldcoin, gdzie w zamian za wyrobienie takiego dowodu otrzymuje się kryptowalutę. Twórcą projektu jest Sam Altman, dyrektor generalny OpenAI – organizacji odpowiedzialnej za stworzenie chatuGPT. Projekt wzbudza kontrowersje, ponieważ nigdy wcześniej dane biometryczne, takie jak tęczówki, nie były przetwarzane na tak szeroką skalę. W niektórych krajach Worldcoin został uznany za potencjalne zagrożenie dla bezpieczeństwa państwowego. Rodzą się pytania o etyczne granice w wykorzystywaniu danych biometrycznych i handlu nimi. Jakie ryzyka wiążą się z takimi praktykami? Czy możliwe jest pogodzenie innowacji technologicznych z ochroną prywatności i bezpieczeństwem danych?

KONTEKST

Nowy projekt Altmana, który w USA zadebiutował w lipcu 2023 roku, ma na celu zmianę sposobu identyfikacji ludzi w sieci oraz stworzenie uniwersalnej waluty cyfrowej. Worldcoin (a właściwie World, bo projekt zmienił nazwę w październiku tego roku) łączy w ramach jednego protokołu open source, cztery elementy: biometrię, sztuczną inteligencję, aplikację blockchain (sterowanie łańcuchem dostaw) oraz kryptowalutę. Projekt oferuje stworzenie World ID, czyli cyfrowego dowodu tożsamości, dzięki któremu łatwiejsze stanie się odróżnienie człowieka od bota, bez ujawniania jakichkolwiek danych osobowych, takich jak imię i nazwisko. World ID mogą uzyskać osoby pełnoletnie, również w Polsce. W Warszawie pojawiły się trzy centra weryfikacji, w których zainteresowane osoby skanują swoje tęczówki oka przez niewielką kulę z obiektywem o nazwie Orb. Na stronie urządzenia czytamy, że jest to "urządzenie, które potwierdza, że jesteś unikalnym człowiekiem". Orb robi zdjęcie twarzy i oczu, a następnie je szyfruje i przechowuje na naszym telefonie. Twórcy zapewniają, że urządzenie nie zatrzymuje jakichkolwiek zdjęć ani innych danych. Celem całego projektu jest odróżnienie człowieka od bota, a jak wskazują twórcy, wraz z rozwojem sztucznej inteligencji, zorientowanie się czy po drugiej stronie komputera znajduje się żywa osoba, będzie stanowić coraz większy problem. Dodatkowo, aby zachęcić do wyrabiania sobie certyfikatów, firma oferuje niewielką ilość kryptowaluty WLD (skrót od nazwy projektu).

Choć przedstawiciele firmy zapewniają, że ich działalność jest zgodna z Rozporządzeniem o Ochronie Danych Osobowych (RODO), budzi ona jednak wiele kontrowersji. Podmiotów prywatnych, które opierają swoje modele biznesowe na niestandardowym przetwarzaniu danych będzie prawdopodobnie przybywało. Wraz z rozwojem systemów sztucznej inteligencji pojawia się coraz więcej rozwiązań, które potrzebują danych biometrycznych. Część z nich wykorzystuje istniejące zbiory do uczenia maszynowego i udoskonalania rozpoznawania obrazów, w tym twarzy, inne projektowane są po to, aby w oparciu o dane tworzyć nowe rozwiązania, wykorzystywane w systemach bezpieczeństwa. Liczba nowych zastosowań będzie się zwiększała, a granice rozwoju wyznaczą nie technologiczne ograniczenia, a regulacje, które stawiają sobie za cel ochronę naszej prywatności. Biorąc pod uwagę wrażliwość danych biometrycznych, a także często inwazyjny sposób ich gromadzenia, zarówno z punktu widzenia ochrony danych, jak i z perspektywy konstytucyjnej. Biometryczne systemy sztucznej inteligencji mogą stanowić zwiększone ryzyko dla ochrony praw podstawowych i zasługują na szczególną uwagę.

BIOMETRIA W CZASACH AI

Zgodnie z publikacją amerykańskiego Narodowego Instytutu Standardów i Technologii (NIST) „Wprowadzenie do bezpieczeństwa informacji", biometrię można zdefiniować jako: „Mierzalną cechę fizyczną lub osobistą, cechę behawioralną używaną do rozpoznawania tożsamości lub weryfikacji deklarowanej tożsamości wnioskodawcy". Technologie oparte na sztucznej inteligencji wykorzystują dane biometryczne takie jak rozpoznawanie twarzy czy skanowanie odcisków palców. Systemy te są powszechnie dostępne w urządzeniach codziennego użytku: telefonach komórkowych i laptopach, gdzie służą m.in. do odblokowywania urządzeń. Odciski palców są wykorzystywane w technologii biometrycznej od ponad wieku. Już w 1892 roku zaczęto stosować je w kryminalistyce, co było możliwe dzięki unikalności wzorów linii papilarnych. Co ciekawe, nie odnaleziono dwóch identycznych odcisków palców – nawet u bliźniąt jednojajowych.

Systemy rozpoznawania twarzy wykorzystują tzw. faceprint, czyli unikalny matematyczny model twarzy. Technologia ta analizuje i mierzy m.in. odległości między oczami, brodą a czołem oraz kształt kości policzkowych, tworząc w ten sposób cyfrowy profil użytkownika. Badanie z 2023 roku przeprowadzone na 10 tysiącach konsumentów z USA, Wielkiej Brytanii, Francji, Niemiec, Australii, Singapuru, Japonii, Korei Południowej, Indii i Chin pokazało, że biometryczne metody weryfikacji cieszą się rosnącą popularnością. Respondenci coraz częściej wolą je od tradycyjnych metod, takich jak hasła czy aplikacje uwierzytelniające.

Kolejnym przykładem wykorzystujący biometrię jest neurotechnologia. Urządzenia neurotechnologiczne są głównie wykorzystywane w medycynie, ale cieszą się coraz

większym zainteresowaniem w marketingu. Urządzenia rejestrują i zbierają dane neuronowe, które odnoszą się do informacji bezpośrednio odzwierciedlających aktywność centralnego lub obwodowego układu nerwowego danej osoby. Mogą ujawniać niezwykle wrażliwe informacje o zdrowiu psychicznym, fizycznym czy ogólnym przetwarzaniu poznawczym.

Wraz z rozwojem nauki i technologii pojawia się coraz więcej rodzajów danych biometrycznych, które potrafimy gromadzić, przetwarzać i używać. Są to zarówno cechy fizyczne, nie tylko odciski palców, kształt twarzy czy tęczówka oka, ale też mniej oczywiste jak kształt uszu, wzory żył czy geometria dłoni. Pojawiają się również zastosowania dla cech behawioralnych, takich jak głos, sposób chodzenia, pisania czy używania urządzeń. Danymi biometrycznymi o coraz większym wachlarzu zastosowań są także unikalne wzorce aktywności serca zobrazowane przez EKG, rozkład temperatury na twarzy (termogram), unikalny skład chemiczny zapachu ciała czy reakcje skórno-galwaniczne na bodźce (badanie pobudzenia). Innymi słowy, współcześnie nasze najbardziej intymne cechy mogą zostać przetworzone przez komputer i wykorzystane przez dostawców usług cyfrowych.

GRANICE TECHNOLOGII

W ostatnich latach szybki rozwój innowacji w zakresie sztucznej inteligencji doprowadził do wzrostu liczby szkód wynikających z działania algorytmów AI. Jest to poważne zagrożenie dla praw obywatelskich i wartości demokratycznych w dzisiejszym krajobrazie technologicznym. System rozpoznawania twarzy, w sklepie Rite Aid w Los Angeles, w celu poprawy wykrywania przestępstw błędnie gromadził wrażliwe dane osobowe i oznaczał mniejszości rasowe jako złodziei sklepowych. Algorytm przewidywania ryzyka przyjęty w celu identyfikacji pacjentów odmówił leczenia osobom czarnoskórym o złym stanie zdrowia, a algorytm mediów społecznościowych mający na celu zwiększenie zaangażowania społecznego zaostrzył zachowania uzależniające i zaburzenia psychiczne u nastolatków. Szkody te stają się coraz bardziej wszechobecne, ale często przejawiają się w małych i niewidocznych formach, umożliwiając ich agregację przy jednoczesnym unikaniu nadzoru regulacyjnego.

Technologie biometryczne wiążą się z podobnymi zagrożeniami. Choć ich zaletą jest możliwość budowania solidnych systemów identyfikacji, to niewłaściwe wykorzystanie tych technologii może prowadzić do poważnych konsekwencji, w tym zagrożenia życia. Informacje biometryczne, ze względu na swoją naturę, są łatwe do wykorzystania w identyfikacji. Do rozpoznania danej osoby nie są potrzebne takie dane osobowe jak imię i nazwisko – wystarczy na przykład zeskanowanie tęczówki oka. Wysoka precyzja i jakość informacji przechowywanych w biometrycznych bazach danych mogą zostać użyte w sposób nieetyczny lub niebezpieczny. Dobitnym przykładem jest sytuacja w Afganistanie,

gdzie talibowie zatrzymali autobus w prowincji Kunduz i przeprowadzili skanowanie biometryczne pasażerów. Osoby zidentyfikowane jako członkowie Afgańskich Sił Obrony Narodowej zostały wytropione i zabite.

Ocena prawdopodobieństwa wystąpienia ryzyka związanego z technologią biometryczną jest złożona i zależy od kontekstu. Kluczowe są czynniki takie jak możliwość niewłaściwego wykorzystania danych przez podmioty mające do nich dostęp czy ryzyko naruszenia danych w systemie. W Afganistanie, gdzie po wycofaniu wojsk amerykańskich istniało wysokie prawdopodobieństwo przejęcia władzy przez talibów, ryzyko niewłaściwego użycia danych było znaczące. Natomiast w krajach z silnymi instytucjami demokratycznymi, które skutecznie rozliczają urzędników, to prawdopodobieństwo jest mniejsze. W związku z tym ryzyko związane z biometrią należy oceniać indywidualnie dla każdego kraju, uwzględniając jego własne uwarunkowania.

PRYWATNOŚĆ NA SPRZEDAŻ?

Podczas gdy w Europie prywatność danych jest fundamentalnym prawem zapisanym w Karcie Praw Podstawowych Unii Europejskiej, w USA prywatność danych nie jest traktowana jako uniwersalne prawo podstawowe. Dlatego tam, priorytet może być częściej przyznawany innowacjom technologicznym i rozwojowi biznesowemu. W porównaniu z europejskim Ogólnym Rozporządzeniem o Ochronie Danych (RODO), amerykańskie podejście do ochrony danych biomedycznych jest bardziej zróżnicowane i zależne od specyficznych przepisów sektorowych oraz stanowych. Podczas gdy RODO ustanawia jednolite standardy ochrony danych osobowych we wszystkich państwach członkowskich UE, w USA brak jest jednolitego, ogólnokrajowego prawa dotyczącego ochrony danych osobowych, co prowadzi do pewnych luk w ochronie i różnic w egzekwowaniu przepisów. W Unii Europejskiej dodatkową ochronę i bezpieczeństwo danych medycznych w tym także biomedycznych zapewniają akt w sprawie zarządzania danymi (Data Governance Act), akt w sprawie danych (Data Act) i dyrektywa w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii (znana jako NIS2).

Europę i USA różni też zaufanie społeczne Na naszym kontynencie ludzie są bardziej świadomi swoich praw związanych z ochroną danych i częściej wykazują sceptycyzm wobec udostępniania danych, np. danych biomedycznych dużym korporacjom. W USA jest zauważalnie większe przyzwolenie na udostępnianie danych w zamian za dostęp do usług technologicznych, choć rośnie świadomość na temat ryzyka związanego z prywatnością. Różnice w kulturze i zaufaniu publicznym między Europą a USA w kontekście przetwarzania danych biomedycznych wynikają z odmiennych tradycji prawnych, poziomu świadomości obywateli oraz podejścia do ochrony prywatności.

CZY KORZYŚCI PRZEWYŻSZAJĄ RYZYKO?

Systemy biometryczne oparte na sztucznej inteligencji zazwyczaj wykorzystują duże zbiory danych treningowych, które umożliwiają im "uczenie się" i tworzenie modeli matematycznych. Na przykład tysiące nagrań głosowych mogą zostać oznaczone jako "w depresji" lub "nie w depresji", a na tej podstawie systemy te będą klasyfikować nowe dane. Warto jednak zauważyć, że dane treningowe są często pozyskiwane bez wyraźnej zgody użytkowników, na przykład z platform wideo takich jak YouTube lub – w przypadku biometrycznych modeli predykcyjnych – z wniosków wizowych. Problem pojawia się, gdy modele matematyczne zaprojektowane do konkretnego celu, np. diagnozy psychologicznej w środowisku klinicznym, są stosowane w innych, nieprzewidzianych kontekstach. Przykładem może być użycie takiego modelu jako wykrywacza kłamstw w działaniach organów ścigania lub w kontekście wojskowym. Takie praktyki mogą prowadzić do nadużyć oraz rodzić poważne problemy etyczne i prawne.

Szczególnie niepokojącym zjawiskiem jest kryzys replikacyjny w badaniach nad sztuczną inteligencją. Wiele modeli uczenia maszynowego nie jest w stanie odtworzyć wyników uzyskanych wcześniej przez ich twórców, co podważa wiarygodność twierdzeń dotyczących możliwości sztucznej inteligencji. Ten problem dotyczy również modeli biometrycznych. Dla przykładu, model predykcyjny sepsy opracowany przez platformę zdrowotną "Epic" został poddany replikacji przez niezależnego badacza i okazał się znacznie mniej dokładny, niż twierdzili jego twórcy. Głównym problemem jest brak przejrzystości – kody i dane potrzebne do stworzenia modeli często nie są udostępniane ze względu na licencje i umowy poufności.

W kontekście neurotechnologii szczególną uwagę zwraca problem świadomej zgody. Technologie, takie jak okulografy połączone z interfejsami mózg-komputer (BCI), mogą wspierać rozpoznawanie emocji u osób z niepełnosprawnościami lub w spektrum autyzmu. Nie zawsze jednak osoby te są w stanie wyrazić zgodę w sposób werbalny. Zwolennicy takich technologii argumentują na rzecz koncepcji „zastępczej zgody", twierdząc, że ich użycie może „rehabilitować" ludzi, umożliwiając im ponowne wyrażenie zgody. Jednak, jak zauważa dr Johnathan Flowers, ableistyczne struktury społeczne oferują ograniczone rozumienie zgody w przypadku osób z niepełnosprawnościami. Według niego brak zgody może być wyrażany na wiele sposobów, np. poprzez brak współpracy, opór czy odmowę, które często mają formę niewerbalną. Dodatkowo pozostaje pytanie, czy te rozwiązania rzeczywiście powstają z myślą o potrzebach swoich odbiorców. Największym wyzwaniem dla osób neuroróżnorodnych nie jest trudność w identyfikacji emocji, lecz brak akceptacji społecznej, problemy ze znalezieniem pracy oraz niewystarczające dostosowanie przestrzeni publicznych do ich potrzeb.

Technologie biometryczne znajdują również zastosowanie w zarządzaniu granicami. Zespół D4FLY opracował prototyp korytarza biometrycznego, który wykorzystuje rozpoznawanie obrazu twarzy 3D i analizę sylwetki na podstawie zdjęć wykonanych podczas przechodzenia przez korytarz. System taki usprawnia kontrolę graniczną i zmniejsza kolejki na lotniskach czy w portach. Mimo to, choć technologia może być postrzegana jako niezawodna, jej awarie mogą stanowić poważne wyzwanie. W takich przypadkach odpowiedzialność za podjęcie decyzji spada na strażników granicznych, co nakłada na nich dodatkowe obciążenie i zwiększa niepewność co do skuteczności technologii.

PRZYSZŁOŚĆ PROJEKTU ALTMANA

Tymczasem mimo licznych kontrowersji, dochodzeń prowadzonych przez organy ochrony danych we Francji i Wielkiej Brytanii czy konieczności zawieszenia działań w Hiszpanii, Portugalii i Kenii, Worldcoin kontynuuje rozwój. Miliony użytkowników pozwalają się zeskanować, zwiększając wartość tokena WLD. Jednak niewątpliwie projekt Altmana stoi przed wyzwaniami regulacyjnymi i etycznymi związanymi z gromadzeniem danych biometrycznych. Przyszłość World, jak i innych firm, które opierają swoje modele biznesowe na przetwarzaniu danych biometrycznych będzie zależeć od ich zdolności do dostosowania się do globalnych standardów ochrony danych i zdobycia zaufania użytkowników.

Opracowały:
Patrycja Didyk, Lidia Stępińska-Ustasiak

Bibliografia

- Access Now. (2023). *Bodily harms: Mapping the risks of emerging biometric tech*. Retrieved from https://www.accessnow.org/wp-content/uploads/2023/10/Bodily-harms-mapping-the-risks-of-emerging-biometric-tech.pdf
- Donohue, L. (2024). *Biomanipulation*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4927993
- European Parliament. (2024). *The protection of mental privacy in the area of neuroscience*. Retrieved from https://www.europarl.europa.eu/RegData/etudes/STUD/2024/757807/EPRS_STU(2024)757807_EN.pdf
- Genser, J., Damianos, S., & Yuste, R. (2024). *Safeguarding brain data: Assessing the privacy practices of consumer neurotechnology companies*. Retrieved from https://www.perseus-strategies.com/wp-

content/uploads/2024/04/FINAL_Consumer_Neurotechnology_Report_Neurorights_Foundation_April-1.pdf

- International Working Group on Data Protection in Technology. (2024). *Working paper on facial recognition technology*.
- Lu, S. (2024). *Regulating algorithmic harms*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4949052
- Murray, D. (2024). *Facial recognition and the end of human rights as we know them?*. Retrieved from https://journals.sagepub.com/doi/epdf/10.1177/09240519241253061
- Paolucci, F. (2024). *From global standards to local safeguards: The AI Act, biometrics, and fundamental rights*. Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4929132
- Scientific American. (2019). *Racial bias found in a major health care risk algorithm*. Retrieved from https://www.scientificamerican.com/article/racial-bias-found-in-a-major-health-care-risk-algorithm/
- UK Parliament. (2024). *Biometric data: Misuse, use, and collation*. Retrieved from https://researchbriefings.files.parliament.uk/documents/POST-PN-0731/POST-PN-0731.pdf
- Yang, Y., Borgesius, F., Beckers, P., & Brouwer, E. (2024). *Automated decision-making and artificial intelligence at European borders and their risks for human rights*.
- PubMed. (2024). *Racial disparities in the utilization of health care technologies: A systemic review*. Retrieved from https://pubmed.ncbi.nlm.nih.gov/38344782/
- Worldcoin. (2024). *System certyfikacji Worldcoin w Polsce*. Retrieved from https://www.computerworld.pl/article/3536307/w-polsce-wystartowal-system-certyfikacji-worldcoin.html
- Worldcoin. (2024). *Worldcoin Orb*. Retrieved from https://pl-pl.world.org/orb