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.*