***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* [*agnieszka.juraszczyk@capgemini.com*](mailto:agnieszka.juraszczyk@capgemini.com)

***Kontakt dla prasy:***

*Aleksandra Witkowska*

*+48 693 407 831*

*E-mail:* [*aleksandra.witkowska@linkleaders.pl*](mailto:aleksandra.witkowska@linkleaders.pl)

**Czy AI może wykorzystywać dane bez narażania prywatności?**

**Inteligentne produkty i usługi muszą osiągać kompromis pomiędzy możliwościami rozwoju a zachowaniem prywatności użytkowników.** **Bezpieczeństwo danych jest coraz ważniejsze w dobie sztucznej inteligencji (AI). Dzięki dzisiejszym możliwościom, nawet anonimowe zestawy danych można poddać inżynierii wstecznej w celu zidentyfikowania osób i wyciągnięcia wniosków na temat ich życia prywatnego (co zostało odkryte przez Netflix w 2006 roku). Jakie są nowoczesne rozwiązania tego problemu?**

Aby zbudować i wytrenować systemy oparte o sztuczną inteligencję, od użytkowników wymaga się udostępniania danych na ogromną skalę. Urządzenia medyczne przechwytują dane dotyczące m.in. tętna, diety, genetyki czy historii terapii. Inteligentne urządzenia domowe zbierają informacje o czynnościach, jakie wykonujemy na co dzień w naszych czterech ścianach. Z kolei systemy wspomagania jazdy gromadzą informacje o tym, gdzie się znajdujemy, jak jeździmy i czy przekraczamy ograniczenia prędkości.

Te dane mogą być wrażliwe. By je chronić, stosuje się anonimizację. Problem pojawia się gdy potrzeba deanonimzacji warunkuje skuteczne szkolenie modeli będących podstawą inteligentnych produktów. Stwarza to możliwość ujawnienia prywatnych informacji, a także utraty lub kradzieży danych. Kompromis w zakresie ich udostępniania wywołuje prosty rachunek: im lepsze i precyzyjniejsze modele, tym więcej stoi za nią danych, a co za tym idzie – większe ryzyko dla prywatności. Z drugiej jednak strony, im więcej informacji mają eksperci (i im więcej tych różnorodnych ekspertów jest), tym większą wartość mogą potencjalnie wnieść.

* Ten kompromis jest często przedstawiany jako „możemy prowadzić analizę danych lub zachować prywatność, ale nie jedno i drugie”. Nie zawsze jednak trzeba dokonywać tego wyboru. To dlatego, że małe, skoncentrowane zespoły mogą bezpiecznie pracować stosując nowoczesne rozwiązania i metody posługiwania się danymi w procesach uczenia maszynowego, obliczeń lub analizy danych. Oczywiście im więcej danych jest udostępnianych, tym większa potencjalna korzyść i jednocześnie większe ryzyko – mówi **Edward Gołda, Data Protection Officer w Capgemini Polska.**

**Nowe rozwiązania chroniące prywatność**

Zasady ochrony prywatności są surowe, a użytkownicy inteligentnych narzędzi nie chcą aby ich zaufanie było wystawione na próbę. Firma Deepmind przekonała się o tym w 2017 roku. Aplikacja Streams, wykorzystująca dane brytyjskiego narodowego funduszu zdrowia, zajmowała się szacowaniem ryzyka ostrego uszkodzenia nerek u wybranych pacjentów. Jednak podczas tworzenia aplikacji firmie nielegalnie udostępniono dokumentację medyczną 1,6 miliona pacjentów, nie poddając jej anonimizacji. To narzędzie, które mogło ratować życie, zostało ostatecznie wycofane, ponieważ podczas wykorzystywania danych osobowych do tworzenia inteligentnego produktu zupełnie pominięto kwestię ochrony prywatności. Przy udostępnianiu bazy danych pacjentów, można było zastosować dostępne sposoby wykorzystania danych do tworzenia AI, chroniące prywatność użytkowników. Stosując te nowoczesne metody podczas przekazywania informacji firmie, możliwe było uniknięcie opisanego problemu. Dziś istnieje już cała gama rozwiązań, które sprawdzają się w tym zakresie. Jakie to rozwiązania?

***Uczenie federacyjne:*** *trenowanie modelu na danych przechowywanych na wielu urządzeniach lub serwerach. Taki model uczy się bez usuwania danych z urządzenia lub tworzenia ich kopii. Można to traktować jako „dzielenie się modelem, a nie danymi” oraz tworzenie globalnego systemu, który uczy się od lokalnych.*

***Bezpieczne obliczenia wielostronne:*** *umożliwiają wielu stronom (instytucjom czy badaczom) pracę nad danymi, których nie chcą całkowicie odsłaniać. Zaszyfrowane informacje są udostępniane między uzgodnionym zestawem osób, co umożliwia pracę na zbiorze składającym się z prywatnych danych wszystkich stron, ale bez wglądu we wrażliwe informacje.*

***Szyfrowanie homomorficzne****,**czyli**przetwarzanie danych zaszyfrowanych. Umożliwiłoby to np. znalezienie danych o osobach cierpiących na artretyzm bazując na informacjach z urządzeń technologicznych do noszenia (jak np. opaski mierzące parametry organizmu), przeprowadzenie na nich obliczeń i stworzenie modelu opartego o dane całej badanej grupy, bez odszyfrowywania danych poszczególnych osób.*

***Zaufane środowisko wykonawcze:*** *funkcja sprzętowa, tworząca bezpieczny obszar na urządzeniu, które może samodzielnie wykonywać określone zatwierdzone funkcje (np. nasze smartfony używają ich do uwierzytelniania biometrycznego). Można je skonfigurować do uruchamiania modeli AI na prywatnych danych bez dostępu do tych informacji przez kogokolwiek.*

***Prywatność różnicowa:*** *dodaje do danych losowy szum, który „psuje” punkty danych, ale zachowuje właściwości całego zestawu. Znając typ losowości, nadal można stworzyć dokładny obraz na poziomie grupy. Ale gdyby ktoś ukradł te dane, to nie określi, czy jakikolwiek indywidualny zapis jest dokładny.*

**Jak technologie chroniące prywatność wyglądają w praktyce?**

Metody te zaczynają być wykorzystywane coraz powszechniej w odkrywaniu leków czy choćby spisach powszechnych. Laboratorium UN PETS (technologie zwiększające prywatność) testuje szereg powyższych rozwiązań, aby umożliwić krajowym urzędom statystycznym, naukowcom i firmom współpracę w zakresie wspólnych danych. Mimo to, ścieżka nie jest prosta. Technologie chroniące prywatność wiążą się z kompromisami. Dostępne techniki często wymagają zaawansowanych obliczeń. Zasłaniając dane celem ochrony prywatności, w niektórych przypadkach tracimy dokładność. Żadna technika nie jest idealna. Zachowanie prywatności będzie wymagało kompromisów i łączenia oraz mieszania technologii dla każdego przypadku.

* Technologie chroniące prywatność nie powinny być dodatkiem, ale podstawową częścią projektu. Każdy proces, który musi udostępniać prywatne dane, powinien opierać się przede wszystkim na ich ochronie. Technologie chroniące prywatność, wdrażane od pierwszych chwil, mogą pomóc przekonać klientów i znaleźć kompromis między poszanowaniem prywatności a maksymalizacją dostępu do użytecznych informacji. Technologie zwiększające prywatność, w tym różnicowa prywatność, federacyjne uczenie się i szyfrowanie homomorficzne są oczywiście trudne do wdrożenia, ale wyspecjalizowane firmy takie, jak Capgemini, pomagają klientom w tym zakresie – dodaje **Edward Gołda.**

Oczywistym celem jest lepsze wykorzystanie danych, które jako społeczeństwo gromadzimy. Szersze, głębsze i bardziej reprezentatywne dane pozwalają tworzyć dokładniejsze, dające się uogólnić, użyteczne modele. Te z kolei stanowią podstawę inteligentnych i spersonalizowanych produktów i usług. Wdrożenie nowych modeli może być trudne i kosztowne, ale oznacza to ochronę i poszanowanie prywatności osób, które udostępniają swoje dane, a w konsekwencji – pozwala na postęp technologiczny i budowę inteligentnych rozwiązań usprawniających życie i funkcjonowanie społeczeństwa.

**O Capgemini**

Capgemini to światowy lider w dziedzinie doradztwa w zakresie transformacji i zarządzania biznesem poprzez wykorzystanie mocy technologii. Celem Grupy jest dążenie do odpowiedzialnej społecznie, zintegrowanej i zrównoważonej przyszłości, w której potencjał ludzki jest wspierany nowymi technologiami. Capgemini jest odpowiedzialną i wielokulturową organizacją, liczącą ponad 350 000 pracowników zatrudnionych w ponad 50 krajach. Dzięki silnemu 55-letniemu dziedzictwu i szerokiej wiedzy branżowej cieszy się zaufaniem swoich klientów, a także jest zdolna kompleksowo zaspokoić ich potrzeby biznesowe: od strategii i projektowania rozwiązań po działania operacyjne napędzane przez dynamicznie rozwijający się i innowacyjny świat technologii chmury, danych, sztucznej inteligencji, łączności, oprogramowania, inżynierii cyfrowej i platform. W 2021 roku Grupa odnotowała globalne przychody w wysokości 18 miliardów euro.

Get The Future You Want | [www.capgemini.com](http://www.capgemini.com/#_blank)