***Kontakt dla prasy:***

*Agnieszka Juraszczyk*

*+48 883 357 638*

*E-mail:* *agnieszka.juraszczyk@capgemini.com*

***Kontakt dla prasy:***

*Aleksandra Witkowska*

*+48 693 407 831*

*E-mail:* *aleksandra.witkowska@linkleaders.pl*

**Sztuczna inteligencja a bezpieczeństwo danych, zasady poszanowania prywatności oraz społeczeństwa**

Komentarz ekspercki Macieja Sowy, Director Intelligent Automation Practice, EMEA Delivery Portfolio Lead w Capgemini Polska

**Sztuczna inteligencja (AI) odgrywa kluczową rolę we współczesnym społeczeństwie. Żyjemy w czasach cyfryzacji firm, a sami jesteśmy użytkownikami najnowszych technologii na co dzień. AI prowadzi samochody, rozpoznaje obrazy, rozumie języki i steruje złożonymi maszynami przemysłowymi. Jednak te systemy podejmowania decyzji mogą mieć wady, które należy zidentyfikować i rozwiązać na etapie projektowania, w przeciwnym razie mogą prowadzić do strat ekonomicznych i utraty zaufania społecznego do sztucznej inteligencji.**

W Capgemini tę nową erę transformacji nazywa się „inteligentnym przemysłem” lub „Przemysłem 4.0”. Inteligentny przemysł polega na wspieraniu synergii między światem cyfrowych procesów biznesowych i fizycznych procesów produkcyjnych, aby pomóc firmom w tworzeniu inteligentnych produktów, operacji i usług na dużą skalę. Jest to era zależna od oprogramowania, napędzana danymi i zdefiniowana przez zrównoważony rozwój oparty na technologii. Od umożliwienia klientom z branży motoryzacyjnej wyboru i zainstalowania funkcji, które mają na celu poprawę wrażeń użytkownika, przez umożliwienie przełomowego podejścia do odkrywania leków w naukach przyrodniczych, po znaczne ograniczenie odpadów i emisji gazów cieplarnianych w operacjach produkcyjnych — to era, która oferuje niezwykły zakres możliwości, ale niesie ze sobą także ryzyko, na które musimy dziś odpowiadać.

**Potrzeba wytycznych i regulacji**

W ciągu ostatnich kilku lat liczba interakcji bezdotykowych z organizacjami zarówno z sektora publicznego, jak i prywatnego wzrosła wykładniczo, a pandemia dodatkowo napędziła ten wzrost. Doświadczenie, które zdobyliśmy podczas kwarantanny i pracy zdalnej, wywołało zwiększenie zainteresowania wykorzystaniem AI w celu usprawnienia operacji biznesowych i produktywności. Wraz ze wzrostem tempa wdrażania rozwiązań AI łatwo było przeoczyć etyczne aspekty sztucznej inteligencji. W odpowiedzi nastąpił silny globalny ruch wokół przepisów dot. AI, który w nadchodzących latach będzie nadal cieszył się dużym zainteresowaniem.

Organy regulacyjne muszą położyć nacisk na opracowanie kryteriów odporności dla systemów sztucznej inteligencji o znaczeniu krytycznym dla bezpieczeństwa oraz metod sprawdzania, czy takie kryteria są spełnione. Należy stworzyć znormalizowane ramy testowania, oceny i audytu, aby wspierać rozwój systemów autonomicznych z myślą o bezpieczeństwie społeczeństwa i operacji biznesowych.

Zaproponowany przez Komisję Europejską w kwietniu 2021 r. projekt rozporządzenia o sztucznej inteligencji to chyba jedna z najbardziej znanych regulacji. Jego celem jest wymuszenie etycznego i bezpiecznego korzystania ze sztucznej inteligencji poprzez kategoryzację rozwiązań AI na podstawie poziomu ryzyka. Zagrożenia te rozciągają się od niedopuszczalnego i wysokiego ryzyka do zastosowań o niższym ryzyku, w zależności od skali i poziomu wpływu na społeczeństwo. W Polsce o rok wcześniej, w 2020 roku, został opublikowany dokument “Polityka dla rozwoju sztucznej inteligencji w Polsce od roku 2020”, który rozpatruje kwestie bezpieczeństwa danych.

**Bezpieczeństwo danych musi być wpisane w pracę twórców AI**

Wraz z rozwojem sztucznej inteligencji, wzrasta zapotrzebowanie na dane, które dziś jest większe niż kiedykolwiek wcześniej i w większości napędzane przez konsumentów. Jednak szansa na większą swobodę, jaką dają łatwo dostępne dane, niesie ze sobą ryzyko dla ich ochrony i prywatności. Dla przykładu – długie umowy mogą skłaniać konsumentów do kliknięcia „akceptuj” bez sprawdzania, jakie dokładnie prawa nadają administratorowi danych. Firmy mogą z kolei wprowadzać dane konsumentów i dostawców do zaawansowanych algorytmów opartych na sztucznej inteligencji. Rozpoznawanie twarzy, systemy identyfikacji głosu i inteligentne urządzenia domowe zbierają dane o tym, kiedy przychodzimy i wychodzimy z domu. Chociaż wiele takich funkcji zapewnia przydatne usługi, potencjalne ryzyko, jakie niosą ze sobą, nie jest trywialne: pozornie anonimowe dane mogą zostać zdeanonimizowane przez sztuczną inteligencję. Zebrane informacje mogą również umożliwić śledzenie, monitorowanie, profilowanie osób i przewidywanie ich zachowań. Podnosząc analizę danych osobowych do nowych poziomów mocy i szybkości, sztuczna inteligencja zwiększa naszą zdolność do wykorzystywania – i nadużywania – danych osobowych, stanowiąc wyzwanie dla prywatności i ochrony danych.

Bezpieczeństwo i prywatność są fundamentalnymi składowymi projektu rozwiązania, gdzie zagrożenia wynikają z samego wdrożenia (limitacji technologicznych lub błędnych założeń). Dlatego pracując nad rozwiązaniami opartymi o sztuczną inteligencję, firmy muszą wdrażać wszystkie niezbędne środki, by przyczynić się do realizacji celów AI klientów w zakresie zgodności z przepisami dotyczącymi prywatności, ochrony danych i właściwego zarządzania nimi. Sztuczna inteligencja i ochrona danych są kompatybilne, o ile ochrona danych i cyberbezpieczeństwo są brane pod uwagę na etapie projektowania każdego wdrożenia AI. Oprócz zapewnienia pełnego poszanowania przepisów i regulacji, należy również wprowadzić odpowiednie mechanizmy zarządzania danymi. Już dzisiaj przedsiębiorstwa opracowujące rozwiązania oparte o AI mogą ograniczać ten nowy rodzaj ryzyka poprzez ograniczenie miejsca procesowania danych wyłącznie do urządzenia lub całkowicie zastąpienia danych potrzebnych do projektu dzięki tak zwanym danymi syntetycznymi (tj. sztucznie przygotowanymi na potrzeby projektu). Kluczowym jest rozwój nowych modeli cyberbezpieczeństwa jak prywatność różnicowa (ang. differential privacy) pozwalającej na gromadzeniu i analizie dużych zbiorów danych bez zawarcia informacji o osobach. W praktyce oznacza to, że każdy projekt AI musiałby zapewniać, że gromadzone i przetwarzane są tylko dane, które są absolutnie niezbędne. W rzeczywistości muszą być one proporcjonalne, dokładne i przetwarzane w bezpieczny sposób. Osoby fizyczne muszą otrzymywać odpowiednie informacje o sposobie przetwarzania ich danych i należy im zapewnić odpowiednie środki do wykonywania przysługujących im praw, zgodnie z wymogami regulacyjnymi.

**Czy społeczeństwo powinno zaufać sztucznej inteligencji?**

Inteligentne algorytmy odgrywają znaczącą rolę we wszystkim, od najprostszych zakupów po to, jak bronimy granic państwowych. Duże postępy w zakresie mocy obliczeniowej i przechowywania danych, w połączeniu ze zwiększoną cyfryzacją procesów, które wcześniej były analogowe, napędzają bezprecedensowy rozwój rozwiązań z zakresu sztucznej inteligencji. Podczas gdy większość twierdzi, że postępy te przyniosły znaczne korzyści społeczeństwu, wiele osób jest zaniepokojonych etycznymi konsekwencjami podejmowania decyzji przez maszyny. Zapewnienie bezpiecznego i etycznego działania rozwiązań z zakresu AI jest istotną troską zarówno firm korzystających z tych rozwiązań, jak i ogółu społeczeństwa. Oznacza to, że należy stworzyć niezbędne środowisko zarządzania i kontroli rozwiązań AI, aby zapewnić bezpieczny i etyczny stan dla wszystkich części składowych.

Budowanie bezpieczniejszych systemów sztucznej inteligencji jest najważniejszym wyzwaniem, przed którym dziś stoimy. Badania Instytutu Badawczego Capgemini dotyczące etyki w sztucznej inteligencji pokazują, że w czasie pandemii 60 proc. organizacji zostało poddanych kontroli prawnej, a 22 proc. spotkało się z reakcją klientów z powodu decyzji podjętych przez ich systemy sztucznej inteligencji.[[1]](#footnote-1) Kwestie bezpieczeństwa mogą poważnie zachwiać zaufaniem do technologii – szczególnie wdrażanej głownie, aby osiągnąć efekt marketingowy. Chociaż w tworzenie bardziej zrozumiałych, przejrzystych i solidnych systemów AI włożono już bardzo wiele pracy, organizacje i organy regulacyjne już teraz podejmują wstępne kroki w celu zaadresowania tych wyzwań – efekty tych prac legislacyjnych możemy odczuć już wkrótce.

**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)

1. *AI and the Ethical Conundrum*, Capgemini 2020 [↑](#footnote-ref-1)