

Czatu GPT konflikty z prawem

29 kwietnia 2023

Nie trzeba było długo czekać, żeby obok memów z papieżem wygenerowanych przez ChatGPT w sieci zaroilo się od treści zawierających manipulację i dezinformację. Aplikacja szybko „weszła” też w konflikt z prawem.

Za pierwszym razem chodziło o prawo autorskie. Wkrótce pojawiło się kolejne pytanie: „Czy ChatGPT będzie objęty przygotowywaną właśnie w Unii Europejskiej regulacją sztucznej inteligencji (AI Act)”? I wtedy włoski urząd ochrony danych wyciągnął asa z rękawa – stwierdził, że narzędzie może naruszać RODO. Problemem zainteresowały się urzędy w Niemczech i Hiszpanii, a [Europejska Rada Ochrony Danych powołała specjalny zespół roboczy](#). Przyglądamy się sprawie.

Czy to prawda, że ChatGPT przetwarza dane osobowe?

Tak. Do przetwarzania danych doszło już na etapie tworzenia bazy, na której później trenowano narzędzie – jeszcze zanim ChatGPT został udostępniony zainteresowanym. Przetwarzaniem jest też etykietowanie danych, czyli przypisywanie im oznaczeń, na przykład na etapie trenowania modelu.

Dane wygenerowane przez program to również dane osobowe: zarówno te prawdziwe, jak i fikcyjne. Danymi osobowymi są też wszystkie informacje wprowadzane do aplikacji przez użytkowników i użytkowniczki w formie tzw. promptów.

ChatGPT przetwarza moje dane. I co z tego?

Przetwarzanie danych osobowych wymaga spełnienia konkretnych warunków. W związku z przetwarzaniem twoich danych:

- należy ci się informacja, w jakich celach są one przetwarzane i na jakiej podstawie prawnej;
- możesz zażądać kopii swoich danych, ich sprostowania lub usunięcia;
- możesz sprzeciwić się przetwarzaniu informacji o tobie, jeśli nie zgadzasz się z celem przetwarzania;
- należy ci się również informacja, jeśli dane podlegają zautomatyzowanemu przetwarzaniu – możesz sprzeciwić się automatycznie podjętej decyzji, która cię dotyczy.

W przypadku programu ChatGPT te warunki nie zostały spełnione.

Przede wszystkim nie wiemy, jak OpenAI pozyskała dane osobowe do wytrenowania modelu ani na jakiej podstawie prawnej je przetwarzała. Być może wykorzystała tzw. uzasadniony interes. Problem w tym, że to nie wystarczy. Jeśli przetwarzane są dane wrażliwe (np. dane ujawniające pochodzenie etniczne czy dane biometryczne) – potrzebna jest zgoda osoby, której dane są przetwarzane (inne podstawy przetwarzania danych wrażliwych są w tym przypadku całkiem nieadekwatne). Uzasadniony interes nie wystarczy też do przetwarzania danych osób poniżej 13 roku życia (na to niezbędna jest zgoda opiekunów prawnych).

Pojawiają się głosy, że osoby, których dane są przetwarzane, powinny być zapytane o zgodę na taki sposób przetwarzania danych. Powinny być o nią pytane za każdym razem, kiedy chat wykorzystuje informacje o użytkownikach do generowania treści. Jesteśmy bardzo ciekawi, jak rozstrzygną to organy ochrony danych!

Wątpliwości budzi też to, czy podmioty danych zdołają skorzystać z przysługującego im prawa do sprzeciwu wobec przetwarzania i poprawienia błędnych danych. Czy gdyby papież złożył wniosek o skorygowanie błędnych danych lub usunięcie głośnego mema z „papieżem Franciszkiem w kurtce zimowej”, doczekałby się spełnienia tego żądania?

Prawo do prywatności – czyli decydowania o tym, jakie informacje o tobie ujrzą światło dzienne i co z tymi informacjami robią różne podmioty – jest jedną z uniwersalnych wartości ujętych w katalogu praw podstawowych. To kluczowy aspekt wolności. Prawo to może być ograniczane, ale tylko w wyjątkowych, uzasadnionych przypadkach. Potrzeby prywatnego biznesu, choćby najbardziej innowacyjnego, nie są takim przypadkiem.

Jak skorzystać z praw, które daje RODO, wobec programu ChatGPT?

Jeśli chcesz skorzystać z praw, które daje ci RODO, wobec programu ChatGPT, zwróć się bezpośrednio do administratora danych, czyli firmy OpenAI. [Zgodnie z polityką prywatności firmy](#), możesz to zrobić przez swoje konto OpenAI lub wysyłając e-mail na adres dsar@openai.com.

Czego możesz zażądać?

- Jeśli chcesz wiedzieć, jakie twoje dane przetwarza firma,awnioskuj o kopię danych.
- Jeśli nie chcesz, żeby ChatGPT przetwarzał twoje dane, wyraż sprzeciw.
- Jeśli uważasz, że ChatGPT wypisuje o tobie głupoty, skorzystaj z prawa do modyfikacji danych lub prawa do zapomnienia.
- Jeśli firma nie zrealizuje twojego żądania w sposób satysfakcjonujący, możesz złożyć skargę do Prezesa Urzędu Ochrony Danych Osobowych ([jak? – dowiesz się TUTAJ](#)).

Jeśli firma OpenAI nie zagwarantuje możliwości uprawnień płynących z RODO, naraża się na karę w wysokości nawet 4% rocznego obrotu.

W przypadku modelu AI działającego w oparciu o sieci neuronowe usunięcie danych konkretnej osoby może okazać się niemożliwe. Co wtedy? Trenowanie modelu od nowa czy usunięcie danych osobowych tylko z wyników? Mamy nadzieję, że odpowiedzi na te pytania pomoże znaleźć specjalna grupa robocza ER0D. I że dzięki interwencjom organów ochrony danych zyskają firmy, które na poważnie podchodzą do ochrony danych osobowych i projektują swoje AI odpowiedzialnie (tak, takie też istnieją!).

Jeśli nie RODO, to co? AI Act!

Już niedługo zostanie przyjęte nowe europejskie prawo regulujące sektor AI: akt o sztucznej inteligencji (AI Act). Panoptikon wraz z europejską koalicją organizacji broniących praw cyfrowych (European Digital Rights, EDRi) zabiega o to, żeby w AI Act znalazły się przepisy chroniące ludzi przed szkodliwym wykorzystaniem technologii.

Walczymy m.in.:

- o to, żeby prawo zakazywało stosowania najbardziej ryzykownych narzędzi opartych na AI, np. systemów oceny społecznej, systemów indywidualnej predykcji kryminalnej;
- o zabezpieczenie ludzi przed dyskryminacją, np. w dostępie do usług, administracji;
- o ograniczenie inwigilacji, do której może dochodzić np. w związku z wykorzystaniem opartej na AI biometrii do kategoryzacji osób ze względu na cechy wrażliwe czy manipulacji opartej na technikach podprogowych;
- o większe uprawnienia dla obywateli, żeby mogli dochodzić swoich praw, oraz wprowadzenie wymogu transparentności systemów AI – szczególnie w obszarach wysokiego ryzyka.

W jaki sposób AI Act uchroni ludzi przed szkodliwym wykorzystaniem narzędzi jak ChatGPT?

Toczy się dyskusja o tym, żeby systemy sztucznej inteligencji ogólnego przeznaczenia, do których należy m.in. ChatGPT, zostały potraktowane w AI Act jako osobna kategoria. Kategoria ta, nazwana roboczo General Purpose AI lub Foundational Models (Modele podstawowe, GP AI), miałyby objąć systemy, które:

- zostały wytrenowane na dużych zbiorach danych;
- zostały zaprojektowane do osiągania ogólnych wyników lub rezultatów (np. generowania treści, analizy dokumentów);
- można je stosować w szerokim zakresie zadań.

Natomiast producenci (dostawcy) narzędzi, które trafią do kategorii GP AI, będą musieli m.in.:

- wykazać, że na etapie projektowania przeanalizowano system pod kątem zagrożeń dla zdrowia, bezpieczeństwa, praw podstawowych, środowiska, demokracji i praworządności oraz zapewniono środki zaradcze w stosunku do tego rodzaju ryzyka;
- zapewnić zgodność z prawem danych wykorzystanych w procesie trenowania modelu;
- jeśli system ma być modyfikowany lub udostępniany – przekazać podmiotom modyfikującym szczegółowe informacje techniczne i instrukcje oraz współpracować przy ewentualnych procedurach kontrolnych.

W przypadku gdy treści generowane przez narzędzie sztucznej inteligencji ogólnego przeznaczenia będą niosły za sobą znaczące ryzyko dla zdrowia, bezpieczeństwa lub praw podstawowych, takie narzędzie zostanie objęte dodatkowymi wymogami dotyczącymi m.in. przejrzystości.

Ta propozycja jest już całkiem blisko postulatów Panoptikonu i innych organizacji społecznych zaangażowanych w prace nad aktem o sztucznej inteligencji. Byłaby jednak jeszcze lepsza, gdyby dodano obowiązek audytowania tych systemów i umieszczania ich opisu w publicznie dostępnej bazie systemów wysokiego ryzyka. Nie chodzi o to, żeby utrudniać życie firmom rozwijającym narzędzia sztucznej inteligencji ogólnego przeznaczenia, ale żeby móc wychwycić i rozbroić związane z nimi ryzyka, zanim te się zmaterializują.

Prace nad aktem o sztucznej inteligencji trwają od dwóch lat i są już na finiszu. Termin kluczowych głosowań w Parlamencie Europejskim był już kilkakrotnie przesuwany m.in. ze względu na medialną burzę wokół programu ChatGPT, która uświadomiła decydentom istotny brak w projekcie. AI Act ma rangę rozporządzenia, będzie więc stosowany bezpośrednio we wszystkich państwach członkowskich Unii Europejskiej – po przyjęciu, które (na co liczymy) nastąpi już wkrótce.

Autorstwo: Anna Obem

Współpraca: Dominika Chachuła, Filip Konopczyński, Katarzyna Szymielewicz

Źródło: [Panoptikon.org](https://panoptikon.org)