

Tytuł konkursu: „**Korzystanie z treści deepfake jako forma przetwarzania danych osobowych**”.

Treść kazusu:

Na numery telefonów niektórych studentów Uczelni A zostały przesłane reklamy zawierające zachętę rektora tej uczelni do skorzystania z usług edukacyjnych spółki nie związanej z Uczelnią A. Jak się okazało, materiał wideo zawarty w reklamie zawierał wizerunek oraz głos rektora Uczelni A wygenerowany przez narzędzie sztucznej inteligencji (deepfake).

Po zgłoszeniu sprawy przez studentów, Uczelnia A przeanalizowała sytuację i ustaliła, że:

- (i) Wideo z rzekomym udziałem rektora wyprodukowała spółka AIMedia, prowadząca działalność polegająca na tworzeniu treści marketingowych z wykorzystaniem narzędzi sztucznej inteligencji.
- (ii) Reklama została przygotowana i rozesłana na zlecenie firmy B z branży edukacyjnej, która potrzebowała kampanii reklamowej promującej nową aplikację szkoleniową.
- (iii) Rektor Uczelni A jest osobą publiczną, aktywną w mediach i często występującą publicznie. Firma B z branży edukacyjnej ani AIMedia nie zawarły z nim żadnej umowy ani nie uzyskały jego zgody na wykorzystanie wizerunku. Dane potrzebne do stworzenia deepfake (nagrania wideo i audio) zostały pozyskane z ogólnodostępnych materiałów w internecie.
- (iv) Kampania marketingowa była wspierana przez system sztucznej inteligencji analizujący dane użytkowników (m.in. ich aktywność edukacyjną, historię wyszukiwania) oraz tworzący profile preferencji. Wysyłka reklamy wykonana została na podstawie automatycznej decyzji narzędzia sztucznej inteligencji, po ocenie, czy określone grupy studentów będą podatne na daną treść reklamy (predykcja przewidywanej skuteczności oddziaływania ze względu na profil użytkownika stworzony na bazie jego zachowania). W niektórych przypadkach decyzje te mogły istotnie wpływać na sytuację użytkowników, np. poprzez selektywne prezentowanie oferty edukacyjnej lub ograniczanie dostępu do określonych treści.

Po ujawnieniu sprawy rektor Uczelni A skierował skargę do Prezesa Urzędu Ochrony Danych Osobowych o naruszenie jego prawa do prywatności i przetwarzanie danych osobowych bez podstawy prawnej. AIMedia odpowiedziała, że wykorzystane zostały materiały dostępne publicznie, rektor jest osobą publiczną, wygenerowany materiał ma charakter twórczy i nie stanowi przetwarzania danych osobowych, działanie to mieści się w granicach wolności gospodarczej i wolności słowa, a sama AIMedia działała na zlecenie firmy B. Firma B nie złożyła wyjaśnień.

Oceń, czy w opisanym stanie faktycznym:

- 1) doszło do przetwarzania danych osobowych rektora Uczelni A w rozumieniu przepisów rozporządzenia 2016/679 (RODO), a jeśli tak, to czy AIMedia lub firma B miały podstawę prawną do przetwarzania danych osobowych w ten sposób?
- 2) znajdzie zastosowanie art. 22 RODO dotyczący zautomatyzowanego podejmowania decyzji, w szczególności w kontekście profilowania odbiorców kampanii reklamowej?

- 3) jakie znaczenie dla oceny sytuacji ma rozporządzenie 2024/1689 (akt w sprawie sztucznej inteligencji), w tym obowiązki dotyczące systemów wysokiego ryzyka oraz wymagania dotyczące transparentności (np. oznaczanie treści deepfake)?