Deepfake – zagrożenia i zarys ram prawnych

Deepfake – zagrożenia i zarys ram prawnych - to kolejny artykuł Instytutu LegalTech przy Naczelnej Radzie Adwokackiej z zakresu nowych technologii. Tekst przygotowany przez apl. adw. Dominikę Królik.

Deepfake to technika generowania obrazów, dźwięków lub nagrań wideo, oparta na sztucznej inteligencji - zaawansowanej technologii deep learning. Polega na łączeniu i nakładaniu na siebie nieruchomych lub ruchomych obrazów, filmów lub dźwięków. W efekcie zastosowania deepfake można otrzymać niezwykle realistycznie zmanipulowane obrazy i nagrania, z przekonująco odtworzoną mimiką twarzy, głosem i gestykulacją danej osoby.

W Internecie coraz częściej pojawiają się nieprawdziwe wideo wygenerowane z zastosowaniem tej technologii. Deepfake staje się coraz częstszym narzędziem w rękach internautów, służąc do manipulacji wypowiedzi polityków, tworzenia fałszywych wiadomości głosowych, szantażu, zniesławiania osób czy działania na szkodę przedsiębiorców. Coraz bardziej powszechnym staje się wykorzystywanie wizerunku osób do manipulacji treści pornograficznych, stwarzając tym samym nieodparte wrażenie udziału poszkodowanej osoby w takim klipie audiowizualnym. Zagrożenie wynikające ze stosowania tego algorytmu jest więc wielopłaszczyznowe, a skutki na poziomie psychologicznym, finansowym i społecznym są daleko idące.

Postęp rozwoju technologii wyprzedził ustawodawstwo, tworząc tym samym lukę prawną. Jako profesjonalni pełnomocnicy stajemy przed wyzwaniem ochrony interesów naszych klientów w obliczu braku jednolitych regulacji prawnych, zarówno na płaszczyźnie cywilnej jak i karnej. Odpowiedzialności należy poszukiwać w przepisach prawa autorskiego, cywilnego, karnego, a także prawa ochrony danych osobowych.

W zakresie ustawy o prawie autorskim i prawach pokrewnym wykorzystanie oraz modyfikacja utworów naruszają zarówno prawa autorskie osobiste, jak i majątkowe twórcy oryginalnego obrazu, dźwięku czy nagrania wideo skutkując odpowiedzialnością odszkodowawczą oraz karną. Naruszeniem wymienionej ustawy będzie także rozpowszechniania wizerunku bez zezwolenia osoby na nim przedstawionej.

W tym miejscu płynnie należy przejść do odpowiedzialności za naruszenie dóbr osobistych, uregulowanej w kodeksie cywilnym za naruszenie chociażby prawa do wizerunku, godności, dobrego imienia czy czci, na podstawie której przysługują roszczenia o zadośćuczynienie czy odszkodowanie.

Odpowiedzialność można rozpatrywać także na gruncie ustawy o zwalczaniu nieuczciwej konkurencji (przyp.1). Rozpowszechnianie nieprawdziwych informacji, polegające na manipulacji treściami z zastosowaniem deepfake, może wypełniać znamiona nieuczciwej praktyki rynkowej uregulowanej w przepisach ustawy o przeciwdziałaniu nieuczciwym praktykom rynkowym.

Wreszcie opisane powyżej działania mogą stanowić znamiona czynów zabronionych określonych w kodeksie karnym takich jak przestępstwo zniesławienia, zniewagi, uporczywego nękania, kradzieży tożsamości, groźby karalnej czy publicznego prezentowania treści pornograficznych.

Należy wspomnieć, że w związku z zaawansowaniem technologii za pośrednictwem której dochodzi do wspomnianych cyberataków, sama identyfikacja podmiotu, który zdarzenia z wykorzystaniem deepfake niejednokrotnie jest obarczona poważnymi trudnościami.

Rozwój technologiczny i złożoność odpowiedzialności prawnej zagadnienia wykorzystania sztucznej inteligencji, w tym deepfake niewątpliwie wymaga jednolitej regulacji. Na poziomie unijnym, stosowanie tej technologii jest jednym z przedmiotów wniosku dotyczącego rozporządzenia Parlamentu Europejskiego i Rady ustanawiającego zharmonizowane przepisy dotyczące sztucznej

inteligencji (Akt w sprawie sztucznej inteligencji) z którym można zapoznać się na oficjalnych stronach Unii Europejskiej (EUR-Lex) (przyp.2).

Zrozumienie, czym jest i jak działa technologia deepfake pomaga w identyfikacji zagrożeń z nią związanych. W przypadku podejrzenia użycia powyższej technologii należy sprawdzić autentyczność treści i zachować ostrożność podczas korzystania z Internetu i udostępniania prywatnych informacji.

Korzyści płynące z rozwoju technologii są niepodważalne. Natomiast w ślad za rozwojem technologii muszą nadążać zmiany w prawie oraz z podejściem do korzystania z nowych technologii przez użytkowników.

Warto zapoznawać się z dobrymi praktykami dotyczącymi cyberbezpieczeństwa w celu świadomego i bezpiecznego korzystania z nowych technologii. Dokumentem takim służącym do zabezpieczenia interesów kancelarii, a także do ochrony interesów klientów są „Dobre Praktyki Dotyczące Cyberbezpieczeństwa w Działalności Kancelarii Adwokackich i Pracy Adwokata” przygotowanych przez Instytut LegalTech. Wśród zaleceń znajdziemy tam sposoby zabezpieczania sprzętu elektronicznego, informacji na nim zawartych, w tym zdjęć, a także komunikacji z klientem.

Zastosowanie nawet podstawowych zabezpieczeń może nas uchronić przed wyciekiem informacji, które mogłyby następnie posłużyć do nielegalnych działań, jak np. użycie technologii deepfake w celu stworzenia nieprawdziwego obrazu lub filmu.

Przypisy:

1.A. Michalak, 4.2. Komputerowa modyfikacja właściwości produktu w przekazie reklamowym [w:] Reklama. Aspekty prawne. Nowe wyzwania, red. M. Namysłowska, Warszawa 2022.

2. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (ARTIFICIAL INTELLIGENCE ACT) AND AMENDING CERTAIN UNION LEGISLATIVE ACTS (COM/2021/206 final).

INSTYTUT
LEGALTECH NRA

Deepfake – zagrożenia i zarys ram prawnych