# Od Sharentingu do Cyfrowego Kidnappingu: wizerunek dziecka w dobie AI i deepfake

Posted on 2024-11-29

Pozornie niewinne zdjęcia i filmy zamieszczane w mediach społecznościowych mogą mieć nieprzewidziane konsekwencje. Internetowe platformy, media społecznościowe, sztuczna inteligencja (AI) oraz technologie takie jak deepfake, wprowadzają nas w erę, w której nie tylko łatwo dzielić się treściami, ale i nimi manipulować. Jednym z najnowszych i najszerzej omawianych problemów w ostatnim czasie jest zjawisko „sharentingu", polegające na udostępnianiu wizerunku swoich dzieci w sieci.

Warto pamiętać, że wizerunek, jako dana osobowa, podlega szczególnej ochronie na mocy przepisów RODO. Dlatego Prezes Urzędu Ochrony Danych Osobowych od lat zwraca uwagę na potrzebę świadomego i odpowiedzialnego zarządzania swoim wizerunkiem w przestrzeni cyfrowej. Problem ten został poruszony również w poradniku „Wizerunek dziecka w internecie. Publikować czy nie?", który został przygotowany przez UODO i Fundację Orange.

Jego celem jest podniesienie świadomości na temat ryzyka, jakie niesie za sobą zbyt swobodne udostępnianie wizerunków dzieci w sieci, a także dostarczenie rodzicom i opiekunom praktycznych wskazówek, jak chronić prywatność swoich dzieci w świecie cyfrowym.

# Sharenting – czy na pewno wiemy, co udostępniamy?

Sharenting to zjawisko, które szturmem zdobyło media społecznościowe, stając się częścią codziennego życia wielu rodziców. Sam termin jest połączeniem angielskich słów „share" (dzielić się) i „parenting" (rodzicielstwo), odzwierciedlając modę na udostępnianie zdjęć, filmów i innych szczegółów z życia dzieci w internecie. Co może wydawać się nieszkodliwym sposobem dzielenia się uroczymi momentami i osiągnięciami swoich pociech, niesie ze sobą jednak ryzyka, o których wielu rodziców często zapomina. Czy rzeczywiście kontrolujemy, kto widzi udostępnione materiały? Jedno zdjęcie z pierwszych kroków dziecka czy film z urodzin mogą szybko rozprzestrzenić się po sieci, zyskując dostęp do tysięcy, jeśli nie milionów użytkowników. Wystarczy chwila nieuwagi – brak odpowiednich ustawień prywatności lub publikacja na otwartym profilu – by zdjęcia znalazły się w rękach nieznajomych. Często zapominamy, że udostępniając te materiały, oddajemy część prywatności naszego dziecka, narażając je na nadużycia. Co gorsza, publikowanie takich treści może prowadzić do tzw. cyfrowego kidnappingu, czyli wykorzystania wizerunku dziecka do tworzenia fałszywych kont i materiałów deepfake.

# Cyfrowy Kidnapping – nowe zagrożenie dla prywatności dzieci

Cyfrowy kidnapping, czyli kradzież tożsamości dziecka w świecie wirtualnym, to problem, który narasta w erze nowoczesnych technologii, takich jak sztuczna inteligencja i deepfake. Rodzice, chcąc dzielić się codziennymi chwilami swoich pociech w mediach społecznościowych, często nie zdają sobie sprawy, że mogą przekazać „klucze” do wizerunku dziecka osobom postronnym. Jak wygląda cyfrowy kidnapping w praktyce? Wystarczy kilka zdjęć lub filmików udostępnionych w sieci, by ktoś stworzył fałszywe profile, strony internetowe, a nawet materiały wideo, które prezentują dziecko w innym, często przerażającym lub kompromitującym kontekście.

Dzięki technologii deepfake oszuści mogą generować materiały wizualne, które wyglądają tak realistycznie, że trudno je odróżnić od prawdziwych nagrań. Wyobraźmy sobie film, w którym wizerunek dziecka zostaje „przyklejony” do sceny z nieodpowiednią treścią, na przykład materiału przeznaczonego wyłącznie dla dorosłych. Takie manipulacje mogą prowadzić nie tylko do cyberprzemocy i zastraszania, ale również do głębokich urazów psychicznych i emocjonalnych. Co ciekawe, już teraz pojawiają się przypadki, gdzie zmanipulowane obrazy dzieci wykorzystywane są w reklamach, kampaniach politycznych czy jako narzędzia do wyłudzania danych. Ten problem przestaje być jedynie teoretycznym zagrożeniem, a staje się realnym ryzykiem, które dotyka coraz więcej rodzin na całym świecie. Współczesne technologie nie tylko umożliwiają tworzenie fałszywych treści, ale także utrudniają ich wykrywanie, co sprawia, że cyfrowy kidnapping jest jednym z najbardziej niepokojących zagrożeń, przed którymi stają dzisiejsi rodzice.

# Inne zagrożenia związane z cyfrowym kidnappingiem: Doxxing, Catfishing

Doxxing, czyli ujawnianie prywatnych informacji o osobie bez jej zgody, to jedno z poważniejszych zagrożeń związanych z cyfrowym kidnappingiem. W przypadku dzieci, informacje udostępnione przez rodziców – takie jak adres, szkoła, hobby czy szczegóły codziennych aktywności – mogą być wykorzystane przez osoby o złych intencjach. Przykładem może być ujawnienie lokalizacji dziecka, co naraża je na kontakt z nieznajomymi, cyberprzemoc lub nawet fizyczne niebezpieczeństwo. Ujawnione informacje mogą być też użyte do szantażu rodziny lub rozpowszechniania fałszywych treści w internecie.

Catfishing to inny sposób wykorzystywania zdjęć dzieci. Przestępcy podszywają się pod nie, aby zdobywać zaufanie innych, często również dzieci, w celu uzyskania kompromitujących informacji, zdjęć lub nawet nawiązania kontaktu osobistego. W skrajnych przypadkach takie fałszywe profile są używane do manipulacji emocjonalnej i wyłudzania danych od innych dzieci lub ich rodzin.

Phishing i socjotechnika – zdjęcia i dane osobowe mogą zostać wykorzystane w atakach phishingowych, gdzie przestępcy próbują zdobyć dodatkowe informacje od ofiary. Oszuści tworzą fałszywe wiadomości, podszywając się pod znane osoby, aby wyłudzić hasła lub dane kart kredytowych. Znając prywatne informacje ofiary, przestępcy łatwiej zdobywają jej zaufanie, co zwiększa skuteczność takich ataków.

# Jak chronić wizerunek dziecka w cyfrowym świecie?

1. Przemyśl, zanim opublikujesz: Zanim udostępnisz wizerunek dziecka, zastanów się, kto może mieć dostęp do tej treści. Ograniczaj publikowanie intymnych i kompromitujących materiałów.
2. Korzystaj z ustawień prywatności: Media społecznościowe oferują różne opcje zabezpieczenia postów. Upewnij się, że zdjęcia Twojego dziecka nie są dostępne publicznie, a jedynie dla najbliższej rodziny i znajomych.
3. Rozmawiaj z dzieckiem: dostosuj do jego wieku informacje o prywatności i zagrożeniach w sieci. Wyjaśnij, dlaczego warto być ostrożnym z publikowaniem prywatnych materiałów.
4. Nie taguj i nie oznaczaj miejsc: Unikaj oznaczania lokalizacji i podawania pełnych imion i nazwisk dzieci w postach. To ograniczy możliwości śledzenia dziecka przez osoby niepowołane.
5. Korzystaj z aplikacji do edycji: Zamiast udostępniać wizerunek dziecka, warto zastosować specjalne aplikacje, które pozwalają na rozmycie twarzy lub jej zasłonięcie.
   Kiedy sztuczna inteligencja rozwija się szybciej niż regulacje prawne, rodzice muszą być bardziej świadomi niż kiedykolwiek wcześniej. Zwłaszcza gdy w grę wchodzi wizerunek dzieci, które same jeszcze nie mają pełnej kontroli nad swoją obecnością w sieci. Warto zadać sobie pytanie, czy publikując zdjęcia naszych dzieci jesteśmy pewni, że nie przyczyniamy się do tworzenia cyfrowych kopii ich wizerunku, nad którymi stracimy kontrolę?