



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**

Mirosław Wróblewski

Warszawa,

sygn. DPNT.413.21.2026

**Komendant Miejski Policji
w Krakowie**

Komenda Miejska Policji w Krakowie

Szanowny Panie Komendancie,

w związku z informacjami przekazanymi przez telewizję regionalną oraz media internetowe na temat prowadzonego przez Komendę Miejską Policji w Krakowie postępowania w sprawie stworzenia przez 17-letnią uczennicę jednej z krakowskich szkół średnich przy użyciu sztucznej inteligencji materiału pornograficznego z wykorzystaniem wizerunku młodszej koleżanki¹, działając na podstawie art. 52 ust. 1 ustawy o ochronie danych osobowych^{2,3} **w celu zapewnienia skutecznej ochrony danych osobowych, zwracam się o uwzględnienie przy prowadzeniu postępowań w tego rodzaju sprawach przedstawionej poniżej analizy prawnej dotyczącej bezprawnego przetwarzania danych osobowych przy użyciu technologii „deepfake”.**

Wyrażam przekonanie, że analiza taka może być Państwu pomocna w postępowaniach karnych w sprawach związanych z wykorzystaniem deepfake.

¹ Np. <https://krakow.tvp.pl/93556996/krakow-skandal-w-liceum-17-latka-miala-tworzyc-tresci-pornograficzne-przy-uzyciu-ai>.

² Ustawa z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019, poz. 1781 ze zm.), nazywana dalej u.o.d.o.

³ Zgodnie z art. 52 ust. 1 u.o.d.o. Prezes Urzędu Ochrony Danych Osobowych może kierować do organów państwowych, organów samorządu terytorialnego, państwowych i komunalnych jednostek organizacyjnych, podmiotów niepublicznych realizujących zadania publiczne, osób fizycznych i prawnych, jednostek organizacyjnych niebędących osobami prawnymi oraz innych podmiotów wystąpienia zmierzające do zapewnienia skutecznej ochrony danych osobowych.

W polskim porządku prawnym dotychczas nie stworzono definicji legalnej, która opisywałaby zjawisko „deepfake’ów”. Wobec tego należy posłużyć się definicją, zawartą w artykule art. 3 pkt 60 aktu w sprawie sztucznej inteligencji⁴. Zgodnie z tym przepisem termin „deepfake” oznacza „wygenerowane przez sztuczną inteligencję (dalej również jako SI) lub zmanipulowane przez SI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe”.

Terminem tym określa się również technologię, która wykorzystuje zaawansowane algorytmy uczenia maszynowego do generowania realistycznych, lecz nieprawdziwych i trudnych do wykrycia fałszywych materiałów. Mogą one przedstawiać np. znane osoby w kompromitujących sytuacjach, polityków wygłaszających kontrowersyjne oświadczenia czy ludzi w spreparowanych scenach. To działanie niebezpieczne tym bardziej, że algorytmy technologii deepfake są w stanie stworzyć realistyczne obrazy oraz dźwięki na podstawie niewielkiej próbki. Pozwala ono uzyskać na tyle wiarygodne rezultaty, że trudno je odróżnić od autentycznych zdjęć czy nagrań.

Choć sama ww. technologia wydaje się być neutralna, to łatwy dostęp do niej oraz jej skuteczność powodują, że może być wykorzystana również do celów niezgodnych z prawem, co może w szczególności stanowić naruszanie praw i wolności poszczególnych osób, czy też bezpieczeństwa grup i całych społeczeństw.

Do zagrożeń tych należą m.in.:

- 1) **Naruszenie wizerunku.** Deepfake’i wykorzystujące wizerunek danej osoby bez jej wiedzy i zgody stanowią naruszenie ochrony danych osobowych oraz dóbr osobistych. Osoby te nie mają kontroli nad tym, w jakim kontekście ich twarz czy głos zostaną użyte, co może prowadzić do poważnych konsekwencji osobistych, zawodowych czy społecznych.
- 2) **Kradzież tożsamości.** Deepfake’i ułatwiają podszywanie się pod inne osoby, zwłaszcza w Internecie. Przestępcy mogą wykorzystywać fałszywe nagrania do uwiarygodniania się i wyludzania poufnych danych, haseł czy pieniędzy.
- 3) **Szantaż i nękanie.** Deepfake’i ukazujące osoby w intymnych sytuacjach służyć mogą do ich zastraszania, poniżania, dyskredytowania czy szantażowania.
- 4) **Oszustwa.** Osoby korzystające z tej technologii mogą tworzyć fałszywe nagrania audio, które przypominają realne rozmowy telefoniczne z urzędami, bankami lub innymi instytucjami finansowymi. Takie nagrania mogą sugerować osobie pilną potrzebę przekazania danych osobowych lub pieniędzy. Oszuści za pomocą materiałów audio mogą również podszywać się pod ekspertów i zachęcać do inwestowania w konkretne produkty lub usługi, co może doprowadzić do strat finansowych.

⁴ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2024/1689 z dnia 13 czerwca 2024 r. w sprawie ustanowienia zharmonizowanych przepisów dotyczących sztucznej inteligencji oraz zmiany rozporządzeń (WE) nr 300/2008, (UE) nr 167/2013, (UE) nr 168/2013, (UE) 2018/858, (UE) 2018/1139 i (UE) 2019/2144 oraz dyrektyw 2014/90/UE, (UE) 2016/797 i (UE) 2020/1828 (akt w sprawie sztucznej inteligencji), (Dz.U.UE.L.2024.1689), dalej jako „akt w sprawie sztucznej inteligencji”.

- 5) **Manipulacja behawioralna.** Spersonalizowane deepfake'i mogą służyć do wpływania na zachowania i decyzje osób, np. poprzez dostosowane reklamy czy rekomendacje.
- 6) **Preparowanie dowodów sądowych.** Deepfake'i mogą stanowić zagrożenie dla wiarygodności i integralności dowodów w postępowaniu sądowym.
- 7) **Zagrożenia dla bezpieczeństwa narodowego.** Deepfake'i mogą być wykorzystywane do dezinformacji i propagandy, prowadząc do manipulacji politycznej (w szczególności podczas prowadzenia kampanii wyborczych), polaryzacji społecznej, zamieszek czy konfliktów z użyciem przemocy.

Materiały wytworzone przy użyciu tej technologii mogą służyć do popełniania szeregu przestępstw takich jak: oszustwa, szantaż, nękanie, zniesławienie, czy naruszenie danych osobowych i dóbr osobistych. Na podstawie Kodeksu karnego⁵ deepfake może wypełniać znamiona np. czynu zabronionego kradzieży tożsamości (art. 190a § 2), zmuszania do określonego zachowania (art. 191), rozpowszechnienia wizerunku nagiej osoby bez zgody (art. 191a), publicznej prezentacji lub produkcji, rozpowszechniania, przechowywania i posiadania treści pornograficznych (art. 202), zniesławienia lub zniewagi (art. 212 i 216) lub oszustwa (art. 286).

To, iż poszczególne przepisy prawa, w tym prawa karnego, nie odnoszą się wprost do czynów popełnianych z zastosowaniem technologii deepfake utrudnia, ale nie uniemożliwia ścigania sprawców i skutecznego dochodzenia praw przez ofiary. Dlatego osoby dopuszczające się takich czynów nie powinny pozostawać bezkarne, a osoby, których dane osobowe (np. wizerunek) zostały wykorzystane w fałszywych materiałach, nie powinny być pozbawione możliwości obrony swoich praw, w tym ustalenia sprawców, żądania usunięcia treści, czy uzyskania zadośćuczynienia za poniesione szkody.

Prezes UODO w swojej praktyce coraz częściej spotyka się przypadkami zrealizowania się niektórych z wymienionych powyżej zagrożeń. Przykładem może być sprawa dotycząca wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki oraz zachęcania innych osób do jego zamawiania na platformie Instagram. Działania polegające na wygenerowaniu wizerunku małoletniego w takim kontekście, w jakim uczynili to sprawcy ww. czynu, jest szkodliwe społecznie w stopniu znacznym i zasługuje na reakcję ze strony właściwych organów ścigania. Jest to działanie nie tylko naruszające prywatność pokrzywdzonej osoby małoletniej, ale przede wszystkim rodzące ryzyko naruszenia elementarnych interesów życiowych tej osoby. W ww. sprawie Prezes UODO zawiadomił Policję o możliwości popełnienia przestępstwa⁶.

W ocenie Prezesa UODO działania polegające na bezprawnym wykorzystaniu wizerunku osoby fizycznej w takim kontekście, w jakim uczynili to sprawcy w opisanych powyżej przypadkach, tj. do wygenerowania przy pomocy technologii deepfake nagiej postaci, czy materiału pornograficznego, może zostać uznane za przestępstwo, o którym mowa w art. 107 ust. 1 u.o.d.o.

⁵ Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383).

⁶ Komunikat UODO dot. tej sprawy dostępny jest pod linkiem: <https://uodo.gov.pl/pl/138/3727>.

Zgodnie z tym przepisem, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne albo do ich przetwarzania nie jest uprawniony, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat dwóch, ale jeżeli czyn ten dotyczy szczególnych kategorii danych⁷ – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech. Czyn ten stanowi zatem przestępstwo powszechne, ścigane z urzędu, z oskarżenia publicznego, za które odpowiedzialność ponosi ten, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne.

W takich sprawach mamy bowiem do czynienia z **przetwarzaniem danych osobowych** w rozumieniu rozporządzenia 2016/679⁸. Aby móc legalnie takie dane przetwarzać musi istnieć podstawa prawna do tego, co oznacza, że musi zostać spełniona jedna z przesłanek wymienionych w art. 6 ust. 1 i art. 9 ust. 2 ww. rozporządzenia. Przetwarzanie, w tym upublicznianie, danych osobowych bez podstawy prawnej stanowi zatem naruszenie ww. przepisów.

Niedopuszczalnym przetwarzaniem danych, o którym mowa w ww. art. 107 u.o.d.o., jest w takim przypadku przetwarzanie danych bez podstawy prawnej, gdy nie występuje żadna z przesłanek legalizacyjnych przetwarzania danych określonych w art. 6 ust. 1 i art. 9 ust. 2 rozporządzenia 2016/679⁹, w szczególności, nie uzyskano zgody osoby, której dane dotyczą na przetwarzanie jej danych osobowych. Wówczas w ocenie Prezesa UODO zachowanie sprawcy może wyczerpywać dyspozycję ww. art. 107 u.o.d.o.¹⁰

Zauważenia w tym miejscu wymaga, że **dla wyczerpania znamion czynu, o którym mowa w art. 107 u.o.d.o. nie ma znaczenia, że dane zdjęcie zostało pozyskane z materiałów ogólnodostępnych w sieci internetowej**. Jak wskazuje się bowiem w doktrynie: „Przedmiotem czynności wykonawczej analizowanego przestępstwa są dane osobowe, czyli wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej”¹¹. Nie ma zatem znaczenia, że pozyskany ewentualnie

⁷ Tj. danych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych, danych genetycznych, danych biometrycznych przetwarzanych w celu jednoznacznego zidentyfikowania osoby fizycznej, danych dotyczących zdrowia, seksualności lub orientacji seksualnej.

⁸ Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 4.5.2016, str. 1 ze zm.), dalej jako „rozporządzenie 2016/679”.

⁹ Zob.: M. Gawroński, K. Kloc, Odpowiedzialność karna w świetle polskiej ustawy o ochronie danych osobowych, LEX/el. 2018). Ponadto P. Fajgielski [w:] Komentarz do ustawy o ochronie danych osobowych [w:] Ogólne rozporządzenie o ochronie danych. Ustawa o ochronie danych osobowych. Komentarz, wyd. III, Warszawa 2025, art. 107) wskazał, że: „Warunkiem odpowiedzialności karnej jest sprzeczność działania sprawcy z wymogami określonymi w przepisach rozporządzenia 2016/679”.

¹⁰ Ponadto zauważyć należy, że ww. opisane okoliczności mogą wyczerpywać znamiona czynu określonego w art. 202 § 3 kk, zgodnie z którym, kto w celu rozpowszechniania produkuje, utrwala lub sprowadza, przechowuje lub posiada albo rozpowszechnia lub prezentuje treści pornograficzne z udziałem małoletniego albo treści pornograficzne związane z prezentowaniem przemocy lub posługiwaniem się zwierzęciem, podlega karze pozbawienia wolności od lat 2 do 15. Jak bowiem wskazał Sąd Najwyższy, „*pornografia dziecięca oznacza jakiegokolwiek materiał, który wizualnie przedstawia dziecko uczestniczące w rzeczywistej lub udawanej czynności wyraźnie seksualnej lub jakiegokolwiek przedstawianie narządów płciowych dziecka głównie w celach seksualnych*” (postanowienie SN z 15.01.2020 r., V KK 655/19, por. też postanowienie SN z 18.01.2021 r., IV KK 251/20, LEX nr 3111703).

¹¹ J. Łuczak-Tarka [w:] Ustawa o ochronie danych osobowych. Komentarz, red. D. Lubasz, Warszawa 2019, art. 107.

wizerunek (zdjęcie) pochodzi z materiałów ogólnodostępnych, bowiem dyspozycja przepisu nie wskazuje źródła pochodzenia danych.

Istotne w takich sytuacjach jest natomiast to, że:

- 1) **są to informacje o osobie zidentyfikowanej lub możliwej do zidentyfikowania, a zatem dane osobowe.** Stosownie bowiem do art. 4 pkt 1 rozporządzenia 2016/679 dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane dotyczą”); możliwa do zidentyfikowania osoba fizyczna to osoba, którą można bezpośrednio lub pośrednio zidentyfikować, w szczególności na podstawie identyfikatora takiego jak imię i nazwisko, numer identyfikacyjny, dane o lokalizacji, identyfikator internetowy lub jeden bądź kilka szczególnych czynników określających fizyczną, fizjologiczną, genetyczną, psychiczną, ekonomiczną, kulturową lub społeczną tożsamość osoby fizycznej. Przykładowo, istnieje wysokie prawdopodobieństwo możliwości identyfikacji osób, których wizerunki zostały zmodyfikowane, gdy są uczniami tych samych szkół, do której uczęszczają sprawcy (sprawca) czynu.
- 2) **przerobienie wizerunku (zdjęcia) osoby stanowi operację przetwarzania danych osobowych.** Pojęcie przetwarzania określono w art. 4 pkt 2 rozporządzenia 2016/679 i oznacza ono operację lub zestaw operacji wykonywanych na danych osobowych lub zestawach danych osobowych w sposób zautomatyzowany lub niezautomatyzowany, taką jak zbieranie, utrwalanie, organizowanie, porządkowanie, przechowywanie, adaptowanie lub modyfikowanie, pobieranie, przeglądanie, wykorzystywanie, ujawnianie poprzez przesłanie, rozpowszechnianie lub innego rodzaju udostępnianie, dopasowywanie lub łączenie, ograniczanie, usuwanie lub niszczenie. Jak wskazuje A. Frydrych-Romańska: „uprawniony będzie wniosek, że ustawa o ochronie danych osobowych wprowadza odpowiedzialność karną za bezprawne przetwarzanie danych osobowych zwykłych”¹². Co więcej: „opisywany rodzaj czynu zabronionego może zostać popełniony wyłącznie poprzez działanie polegające na przetwarzaniu danych osobowych, o którym mowa w art. 4 pkt 2 RODO (...). Bezprawne przetwarzanie danych osobowych ma charakter formalny, co oznacza, że do jego popełnienia nie jest wymagane wystąpienie jakiegokolwiek skutku działania sprawcy”¹³. W ocenie Prezesa UODO, przerobienie wizerunku osoby jest przetwarzaniem danych osobowych – dochodzi bowiem do operacji na danych osobowych, zaś sam wizerunek do tych danych niewątpliwie należy.
- 3) **działanie sprawcy (sprawców) jest bezprawne i niedopuszczalne** – jeśli nie dysponował żadną z przesłanek legalizacyjnych przetwarzanie danych określonych w art. 6 ust. 1 i art. 9 ust. 2 rozporządzenia 2016/679, a zatem nie był uprawniony do wykorzystania danych osobowych w postaci wizerunku osoby w żaden sposób, tym bardziej do zmodyfikowania go i dalszego udostępniania.

¹² A. Frydrych-Romańska, Odpowiedzialność karna w świetle ustawy o ochronie danych osobowych, LEX/el. 2023.

¹³ Tamże.

Wyjątkowego podkreślenia wymaga, że **osoby małoletnie** – jako mniej świadome ryzyka, konsekwencji, zabezpieczeń i praw przysługujących im w związku z przetwarzaniem danych osobowych – **powinny być objęte szczególną ochroną**. Co więcej w takich sytuacjach, jak wskazano na wstępie, istnieje wysokie prawdopodobieństwo możliwości identyfikacji, a tym samym też stygmatyzacji, zastraszania, poniżania, czy wyśmiewania. Wizerunek osoby należy do sfery jej prywatności. Jak wskazano w orzecznictwie: »„Prywatność osoby fizycznej” jest pewną sytuacją prawną konkretnego człowieka. Jest to pewna korzystna sytuacja prawna podlegająca ochronie chociażby przez to, że informacje mieszczące się w zakresie pojęcia prywatności nie mogą być co do zasady udostępniane (poza wyjątkami ustawowo określonymi) (...)« (wyrok WSA w Krakowie z 13 maja 2019 r., II SA/Kr 97/19, LEX nr 2684058).

Przywołania również wymaga argumentacja zawarta w ww. wystąpieniu Prezesa UODO (sygn. DPNT.413.31.2025), w którym wskazano, że „technologia deepfake pozwala na dostosowanie różnego rodzaju kontekstów, które sprawiają, że sztucznie stworzone wideo i audio wydaje się autentyczne. W tym celu wykorzystuje się synchronizację mimiki twarzy z dźwiękiem lub innymi czynnikami zewnętrznymi. Pozwala to uzyskać na tyle wiarygodne rezultaty, że trudno je odróżnić od autentycznych zdjęć czy nagrań”. To właśnie trudność w odróżnieniu sztucznie wygenerowanego zdjęcia od takiego, które mogło powstać w rzeczywistości, wpływa na szczególną szkodliwość opisywanego zjawiska i powoduje negatywne skutki nie tylko w wizerunku pokrzywdzonych osób, ale również w ich sferze psychicznej¹⁴.

Powołując się na całokształt przedstawionych powyżej okoliczności bardzo ważne jest aby przestępstwa związane z bezprawnym przetwarzaniem danych osobowych w postaci wizerunku, w tym przy pomocy technologii deepfake, spotykały się ze stanowczą i szybką reakcją organów ścigania. Nikt z nas bowiem nie chciałby, aby jego wizerunek lub wizerunek jego dziecka, znajdujący się w Internecie w związku z realizacją np. obowiązków zawodowych lub zamieszczony na portalu społecznościowym, został bezprawnie wykorzystany w opisany powyżej sposób i upubliczniony, a sprawca aby pozostawał bezkarny.

W ocenie Prezesa UODO zasadne i konieczne jest zatem prowadzenie przez organy ścigania postępowań w takich sprawach, szczególnie zwłaszcza w kontekście ochrony dóbr małoletniej osoby pokrzywdzonej. Brak reakcji organów ścigania na tego typu przestępstwa powodować może, z jednej strony brak świadomości, iż jest to czyn zabroniony, a z drugiej poczucie bezkarności sprawców.

¹⁴ Warto też wspomnieć o zjawisku AI CSAM. „CSAM” to skrót od pierwszych liter wyrazów składających się na angielski termin „child sexual abuse material” oznaczający materiały przedstawiające wykorzystywanie seksualne dzieci. To wszelkie materiały wizualne, w tym między innymi zdjęcia, filmy i obrazy generowane komputerowo, przedstawiające czynności seksualne z udziałem osób małoletnich. Sztucznie wygenerowany CSAM może ponownie wiktymalizować rzeczywiste dzieci, ponieważ ich obrazy są zbierane z Internetu i wykorzystywane za pomocą narzędzi SI do tworzenia nowych obrazów. Więcej informacji na ten temat dostępnych jest w materiale: Prezes UODO interweniuje u Prokuratora Generalnego w sprawie wygenerowania nagiego zdjęcia uczennicy, który dostępny jest na stronie internetowej UODO pod linkiem <https://uodo.gov.pl/pl/138/3984>).

Zwracam się zatem z uprzejmą prośbą o uwzględnianie w postępowaniach prowadzonych w tego typu sprawach, przedstawionej powyżej argumentacji co do konieczności ścigania sprawców bezprawnego przetwarzania danych osobowych przy pomocy technologii deepfake, w szczególności gdy chodzi o dane osób małoletnich.

Łączę wyrazy szacunku

Mirosław Wróblewski

Prezes Urzędu

Ochrony Danych Osobowych