



**PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH**
Miroslaw Wróblewski

Warszawa, 24 marca 2026 r.

DKN.5101.170.2026

**Prokuratura Rejonowa
Warszawa - Śródmieście
ul. Krucza 38/42
00-512 Warszawa**

Zawiadomienie o uzasadnionym podejrzeniu popełnieniu przestępstwa

Na podstawie art. 304 § 2 kpk¹ zawiadamiam o podejrzeniu popełnienia przestępstwa polegającego na przetwarzaniu danych osobowych, choć ich przetwarzanie nie jest dopuszczalne – poprzez umieszczenie pod jednym z postów Pani A na jej koncie w mediach społecznościowych pod nazwą „X” komentarza, w którym ktoś zawarł cyfrowo przerobione zdjęcie kobiety, na którym jest naga – tj. przestępstwa określonego w art. 107 u.o.d.o.².

Uzasadnienie

Prezes Urzędu Ochrony Danych Osobowych (zwany dalej: Prezesem UODO), w myśl art. 34 ust. 1 u.o.d.o., jest organem właściwym w sprawie ochrony danych osobowych.

Zgodnie zaś z art. 57 ust. 1 lit. a) rozporządzenia 2016/679³ każdy organ nadzorczy (którym w Rzeczypospolitej Polskiej jest Prezes UODO) na swoim terenie monitoruje i egzekwuje stosowanie tego rozporządzenia.

¹ Ustawa z dnia 6 czerwca 1997 r. Kodeks postępowania karnego (Dz. U. z 2025 r. poz. 46 ze zm.), zwana dalej „kpk”.

² Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781), zwana dalej: „u.o.d.o.”.

³ 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 4.05.2016, str. 1, Dz. Urz. UE L 127 z 23.05.2018, str. 2 oraz Dz. Urz. UE L 74 z 4.03.2021, str. 35), zwane dalej: „rozporządzeniem 2016/679”.

Stosownie 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.

Pojęcie przetwarzania natomiast określono w art. 4 pkt 2 rozporządzenia 2016/679 i oznacza 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.

Art. 5 ust. 1 lit. a) i c) rozporządzenia 2016/679 stanowi, że dane osobowe muszą być: przetwarzane zgodnie z prawem, rzetelnie i w sposób przejrzysty dla osoby, której dane dotyczą („zgodność z prawem, rzetelność i przejrzystość”), a ponadto: adekwatne, stosowne oraz ograniczone do tego, co niezbędne do celów, w których są przetwarzane („minimalizacja danych”).

Stosownie zaś do art. 6 ust. 1 rozporządzenia 2016/679, przetwarzanie jest zgodne z prawem wyłącznie w przypadkach, gdy – i w takim zakresie, w jakim – spełniony jest co najmniej jeden z poniższych warunków: a) osoba, której dane dotyczą wyraziła zgodę na przetwarzanie swoich danych osobowych w jednym lub większej liczbie określonych celów; b) przetwarzanie jest niezbędne do wykonania umowy, której stroną jest osoba, której dane dotyczą, lub do podjęcia działań na żądanie osoby, której dane dotyczą, przed zawarciem umowy; przetwarzanie jest niezbędne do wypełnienia obowiązku prawnego ciążącego na administratorze; c) przetwarzanie jest niezbędne do ochrony żywotnych interesów osoby, której dane dotyczą, lub innej osoby fizycznej; przetwarzanie jest niezbędne do wykonania zadania realizowanego w interesie publicznym lub w ramach sprawowania władzy publicznej powierzonej administratorowi; d) przetwarzanie jest niezbędne do celów wynikających z prawnie uzasadnionych interesów realizowanych przez administratora lub przez stronę trzecią, z wyjątkiem sytuacji, w których nadrzędny charakter wobec tych interesów mają interesy lub podstawowe prawa i wolności osoby, której dane dotyczą, wymagające ochrony danych osobowych, w szczególności gdy osoba, której dane dotyczą, jest dzieckiem.

Odrębne zasady dotyczą przetwarzania danych osobowych szczególnych kategorii. Zgodnie z art. 9 ust. 1 rozporządzenia 2016/679 zabrania się bowiem przetwarzania danych osobowych ujawniających pochodzenie rasowe lub etniczne, poglądy polityczne, przekonania religijne lub światopoglądowe, przynależność do związków zawodowych oraz przetwarzania danych genetycznych, danych biometrycznych w celu jednoznacznego zidentyfikowania osoby fizycznej lub danych dotyczących zdrowia, seksualności lub orientacji seksualnej tej osoby. Wyjątki od tego ogólnego zakazu przewiduje z kolei art. 9 ust. 2 tego rozporządzenia.

Prezes UODO powziął informację o zdarzeniu opisanym na stronie internetowej: (...), które polegało na umieszczeniu komentarza pod jednym z postów Pani A na jej koncie w mediach społecznościowych pod nazwą „X”, w którym ktoś zawarł cyfrowo przerobione zdjęcie kobiety, na którym jest naga.

Zdarzenie pierwotnie zostało opisane w poście z dnia (...) marca 2026 r. na koncie Pani A, w którym wskazała że, cyt.: *„Moje zdjęcie zostało przerobione (ROZEBRANE) za pomocą AI przez jakiegoś obleśnego typa a następnie umieszczone w internecie - pisze w mediach społecznościowych A, wiceprezesa K. - Czuję się paskudnie, czuję się skrzywdzona i nawet mówienie sobie, że przecież to nie było moje ciało, niewiele pomaga”*

W treści artykułu umieszczonego na portalu C wskazano także, że cyt.: *„Kilka godzin później zamieściła kolejny post, poinformowała zgłosić zdarzenie do odpowiednich służb. Mimo ogromu wsparcia, w komentarzach znalazły się również głosy o tym, że jest grubaską, że kłamie lub czy to bait. Pojawiły się również dywagacje na temat tego, dlaczego ktoś jej to zrobił. Jeden z użytkowników zasugerował nawet, żeby znalazła sobie "gałązkę i linkę”*

Jak stanowi art. 107 ust. 1 u.o.d.o., 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 określony w ust. 1 dotyczy 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 – podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat trzech (ust. 2 ww. artykułu).

Czyn opisany w treści dyspozycji art. 107 ust. 1 u.o.d.o. stanowi przestępstwo powszechne, ścigane z urzędu, z oskarżenia publicznego, za które odpowiedzialność ponosi ten, kto przetwarza dane osobowe, choć ich przetwarzanie nie jest dopuszczalne. Niedopuszczalnym przetwarzaniem danych jest w takim przypadku przetwarzanie danych bez podstawy prawnej, gdy nie występuje żadna z przesłanek legalizacyjnych przetwarzania danych określonych w rozporządzeniu 2016/679 (art. 6 i 9) (patrz: M. Gawroński, K. Kloc, Odpowiedzialność karna w świetle polskiej ustawy o ochronie danych osobowych, LEX/el. 2018). Jednocześnie, jak wskazuje P. Fajgielski: **„Warunkiem odpowiedzialności karnej jest sprzeczność działania sprawcy z wymogami określonymi w przepisach rozporządzenia 2016/679”** (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).

W ocenie Prezesa UODO zachowanie sprawcy wyczerpuje dyspozycję art. 107 u.o.d.o. poprzez przetwarzanie danych osobowych, w sytuacji, gdy jest to niedopuszczalne i nieuprawnione. Przerobienie wizerunku pokrzywdzonej nosi znamię przetworzenia danych osobowych – bowiem doszło do operacji na danych osobowych, a sam wizerunek do tych danych należy. W przedmiotowej sprawie, w ocenie Prezesa UODO nie wystąpiła także żadna z przesłanek legalizacyjnych dla procesu przetwarzania danych (wskazanych w art. 6 i 9 rozporządzenia 2016/679), w szczególności, nie uzyskano zgody osoby, której dane dotyczą na

przetwarzanie jej danych osobowych w jednym lub większej liczbie określonych celów. Już w samym poście umieszczonym na koncie „X” z dnia (...) marca 2026 r. pokrzywdzona wprost wskazała, że „Czuję się paskudnie, czuję się skrzywdzona i nawet mówienie sobie, że przecież to nie było moje ciało, niewiele pomaga”, co potwierdza jednoznacznie brak zgody pokrzywdzonej na takie wykorzystanie jej wizerunku.

Pokreślenia w szczególności wymaga, że wygenerowanie wizerunku pokrzywdzonej w takim kontekście, w jakim uczynił to sprawca czynu, jest szkodliwe społecznie i zasługuje na reakcję ze strony właściwych organów ścigania. Działanie sprawcy nie tylko godzi w prywatność pokrzywdzonej, ale również rodzi ryzyko naruszenia jej elementarnych interesów życiowych. Niepokojące są także reakcje internautów na post pokrzywdzonej, w którym zwraca uwagę na ten problem.

Zwrócić także uwagę należy na sam charakter deep fake’ów i ich wyjątkową szkodliwość. W polskim porządku prawnym dotychczas nie stworzono definicji legalnej, która opisywałaby przedmiotowe zjawisko, co wymusza odniesienie do legislacji unijnej. Definicja deepfake’ów, którą należy się posługiwać, zawarta została w artykule 3 pkt 60 AI Act⁴, zgodnie z którym są to: „wygenerowane przez AI lub zmanipulowane przez AI obrazy, treści dźwiękowe lub treści wideo, które przypominają istniejące osoby, przedmioty, miejsca, podmioty lub zdarzenia, które odbiorca mógłby niesłusznie uznać za autentyczne lub prawdziwe”.

W przedmiotowej sprawie doszło wygenerowania wizerunku pokrzywdzonej bez jej zgody, przy wykorzystaniu jej ogólnodostępnych zdjęć przy wykorzystaniu narzędzi Sztucznej Inteligencji. Zjawisko takie jest odrębną kategorią deep fake’ów, która opisana została w szczególności w publikacji p.t.: „Deep fakes i nadużycia na tle seksualnym – prawo wobec wyzwań syntetycznych mediów”. Kategoria ta nosi nazwę *non-consensual synthetic intimate imagery* (NSII), zaś zgodnie z treścią ww. publikacji, powszechnie takie zjawisko opisywane jest jako *deep porn*, co ma nawiązywać do połączenia terminów *deep fakes* i *pornography*. Autorzy skłaniają się jednak do używania terminu *non-consensual synthetic intimate imagery* (NSII), jako bardziej adekwatnego – tj. takiego który zwraca uwagę przede wszystkim na aspekt abuzywny i niekonsensualne wykorzystanie cudzego wizerunku i obrazów intymnych⁵. Jak autorzy publikacji dalej wskazują, cyt.: „obrazy służące za podstawę syntezy AI mogą być pozyskiwane przez sprawców z dostępnych publicznie źródeł, a brak konsensualności odnosi się przede wszystkim do braku zgody na wykorzystanie wizerunku”⁶. Wyodrębnienie tej kategorii deep fake’ów jest szczególnie istotne z perspektywy opisanych poniżej konsekwencji takiego generowania zdjęć pokrzywdzonych. Jak dodatkowo wskazują autorzy publikacji, „NSII jest dominującym przejawem wykorzystania deep fakes w formie wideo – stanowi ponad 90% z nich. **W blisko 100% przypadków NSII w formie deep fakes dotyka kobiet, co prowadzi**

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 z 12.07.2024) – zwane dalej AI Act.

⁵ M. Łabuz, dr hab. M. Małecki, adw. dr K. Mania, *Deep fakes i nadużycia na tle seksualnym – prawo wobec wyzwań syntetycznych mediów*, https://ceeddw.org/wp-content/uploads/2025/03/DeepFakes_sklad_internet.pdf, s. 9.

⁶ M. Łabuz, dr hab. M. Małecki, adw. dr K. Mania, *Deep fakes i nadużycia na tle seksualnym – prawo wobec wyzwań syntetycznych mediów*, https://ceeddw.org/wp-content/uploads/2025/03/DeepFakes_sklad_internet.pdf, s. 9.

do wiktymizacji tysięcy z nich na całym świecie, a także przyczynia się do wzmacniania stereotypów płciowych oraz uprzedmiotowienia kobiet, wywierając trudny do skwantyfikowania wpływ na społeczeństwo”⁷.

Zwrócić uwagę należy także, że już sama definicja zawarta w AI Act wprost wskazuje na manipulacyjny charakter materiałów, a także na kwestię wykorzystywania wizerunków bez zgody osób pokrzywdzonych, co należy uznać za szczególnie szkodliwe – zwłaszcza dla kobiet. Powtarzając ponownie za autorami opisanej powyżej publikacji dotyczącej deep fake’ów wskazać należy, że cyt.: „Deep fakes stwarzają liczne wyzwania w wielu obszarach. Są m.in. wykorzystywane do wspierania dezinformacji, co stereotypowo łączone jest głównie z potencjałem do manipulacji wyborczych. Ich szkodliwe zastosowania powinny być jednak rozpatrywane znacznie szerzej. **Nie tylko umożliwiają one tworzenie treści fałszywych, które mogą zniszczyć reputację jednostek, ale również są wykorzystywane w cyberprzemocy, w tym szantażach, wymuszeniach oraz szerzeniu przemocy na tle seksualnym, prowadząc do daleko idących konsekwencji społecznych i politycznych, a przede wszystkim wywołując negatywne skutki psychologiczne dla poszkodowanych, z których istotną grupę stanowią kobiety**”⁸.

Przywołania również wymaga argumentacja zawarta w wystąpieniu Prezesa UODO skierowanym do Pana Krzysztofa Gawkowskiego, Wiceprezesa Rady Ministrów, Ministra Cyfryzacji oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa (sygn. DPNT.413.31.2025), w którym wskazano, że cyt.: „**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**”⁹. To właśnie trudność w odróżnieniu sztucznie wygenerowanego zdjęcia od takiego, które mogło powstać w rzeczywistości, ma wpływać na szczególną szkodliwość opisywanego zjawiska i powodować negatywne skutki nie tylko w wizerunku pokrzywdzonych osób, ale również w ich sferze psychicznej.

Podkreślić należy, że generowanie zdjęć i tworzenie deep fake’ów, staje się coraz powszechniejsze. Dotychczas w zainteresowaniu Prezesa UODO znalazło się kilka przypadków nadużyć spowodowanych stosowaniem technologii deep fake, które zostały opisane m.in. w komunikacie na stronie UODO. Prezes UODO zajmował się już sprawami takimi, jak: sprawa skargowa dotycząca zamieszczania na portalach społecznościowych fałszywych informacji odnoszących się do dziennikarki, osoby aktywnej publicznie – o jej śmierci, o tym, że została pobita przez męża czy że trafiła do więzienia; sprawa wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki oraz sygnały od lekarzy, którzy padli ofiarą oszustów korzystających z technologii deep fake – ich

⁷ M. Łabuz, dr hab. M. Małecki, adw. dr K. Mania, *Deep fakes i nadużycia na tle seksualnym – prawo wobec wyzwań syntetycznych mediów*, https://ceeddw.org/wp-content/uploads/2025/03/DeepFakes_sklad_internet.pdf, s. 9.

⁸ M. Łabuz, dr hab. M. Małecki, adw. dr K. Mania, *Deep fakes i nadużycia na tle seksualnym – prawo wobec wyzwań syntetycznych mediów*, https://ceeddw.org/wp-content/uploads/2025/03/DeepFakes_sklad_internet.pdf, s. 7.

⁹ <https://uodo.gov.pl/pl/138/3886>

wizerunki i autorytet zostały wykorzystane w nieprawdziwych reklamach, w których medycy rzekomo zachęcali do przyjmowania określonych preparatów¹⁰. Powyższe wskazuje, że zainteresowanie takim generowaniem plików na szkodę pokrzywdzonych osób wzrasta i powinno spotkać się ze stanowczą reakcją organów ścigania – także w opisywanym w niniejszym zawiadomieniu przypadku.

Informacyjnie przy tym wskazuję, że we wskazanych postach Pani A na portalu X przekazano informację o złożeniu przez nią zawiadomienia do organów ścigania w sprawie przedmiotowego czynu.

Finalnie wskazuję, że zgodnie z art. 304 § 2 kpk, instytucje państwowe i samorządowe, które w związku ze swą działalnością dowiedziały się o popełnieniu przestępstwa ściganego z urzędu, są obowiązane niezwłocznie zawiadomić o tym prokuratora lub Policję oraz przedsięwziąć niezbędne czynności do czasu przybycia organu powołanego do ścigania przestępstw lub do czasu wydania przez ten organ stosownego zarządzenia, aby nie dopuścić do zatarcia śladów i dowodów przestępstwa.

Z uwagi na powyższe zawiadamiam jak na wstępie.

Mirosław Wróblewski

Prezes Urzędu Ochrony Danych Osobowych

¹⁰ Komunikat publiczny, „Potrzebne jest prawo chroniące ludzi przed negatywnym wpływem deepfake’ów” z 18.09.2025 r., <https://uodo.gov.pl/pl/138/3886>