PREZES
URZĘDU OCHRONY
DANYCH OSOBOWYCH
Mirosław Wróblewski

Warszawa,

DPNT.413.31.2025

Pan
Krzysztof Gawkowski
Wiceprezes Rady Ministrów
Minister Cyfryzacji
Pełnomocnik Rządu
ds. Cyberbezpieczeństwa

Szanowny Panie Premierze,

działając na podstawie art. 52 ust. 2 ustawy o ochronie danych osobowych[1] **zwracam się do Pana Premiera z uprzejmą prośbą i wnioskiem o rozważenie wprowadzenia rozwiązań ustawowych, które zapewnią skuteczną ochronę przed negatywnym wpływem deepfake'ów, zwłaszcza osobom fizycznym.**

Przypadki nadużyć spowodowanych stosowaniem technologii deepfake zgłaszane Prezesowi Urzędu Ochrony Danych Osobowych, a także analiza aktualnych regulacji prawnych, uwidoczniają braki systemowe, które w ocenie organu ochrony danych osobowych wymagają pilnego przyjęcia regulacji przeciwdziałających szkodliwemu wykorzystaniu tej technologii. Postęp technologiczny, w tym rozwój sztucznej inteligencji, musi bowiem uwzględniać prawa i bezpieczeństwo obywateli oraz odpowiedzialność instytucji publicznych oraz prywatnych w budowaniu zaufania i odporności społecznej. Wskazuje to na ważną rolę prawodawcy w erze cyfrowej transformacji.

Deepfake'i przyczyniają się do szerzenia się zjawiska dezinformacji, której przeciwdziałanie jest szczególnie potrzebne w czasach podejmowanych różnorakich form ataków ze strony Federacji Rosyjskiej. W pełni popieram ostrzeżenia opublikowane

[1] Zgodnie z art. 52 ust. 2 ustawy z 10 maja 2018 r. o ochronie danych osobowych (Dz. U. z 2019 r. poz. 1781) Prezes Urzędu Ochrony Danych Osobowych może występować do właściwych organów z wnioskami o podjęcie inicjatywy ustawodawczej albo o wydanie lub zmianę aktów prawnych w sprawach dotyczących ochrony danych osobowych.

Urząd Ochrony
Danych Osobowych
ul. Moniuszki 1a
00-014 Warszawa

tel. 22 531-03-88
fax 22 531-03-99

www.uodo.gov.pl

przez Ministerstwo Cyfryzacji[2], w których zwrócono uwagę, że każdy powinien zachować najwyższą ostrożność w związku z informacjami pojawiającymi się w przestrzeni publicznej – szczególnie w mediach społecznościowych, każdorazowo należy weryfikować źródła informacji i nie udostępniać materiałów z niesprawdzonych, nie należy ulegać emocjom, szczególnie widząc publikacje ze zdjęciami czy materiałami wideo, które mogą być sfałszowane lub obrazować zupełnie inne sytuacje niż sugerują opisy.

Termin „deepfake” został zdefiniowany w art. 3 pkt 60 aktu w sprawie sztucznej inteligencji[3] i 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.

Tworzenie fałszywych obrazów lub nagrań z wykorzystaniem SI zaczyna się od zebrania danych treningowych, w postaci plików wideo, nagrań głosu lub zdjęć ludzkiej twarzy, które umożliwiają sztucznej inteligencji zapoznanie się z mimiką, sposobem mówienia oraz innymi cechami danej osoby. Następnie algorytm – przy wykorzystaniu oryginalnego materiału – dąży do stworzenia jak najbardziej zgodnego z rzeczywistością obrazu i dźwięku, na którym fikcyjna postać imituje to, jak wygląda lub mówi konkretna osoba.

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.

Choć sama ww. technologia wydaje się być neutralna, to łatwy dostęp do niej oraz jej skuteczność w wykorzystaniu dla różnych celów budzą poważne obawy**. Deepfake niesie ze sobą zarówno szanse** na postęp technologiczny, który może być wykorzystany w pozytywny sposób (np. tworzenie efektów specjalnych w filmach), **jak i groźbę nadużyć i naruszania praw i wolności ludzi na niespotykaną dotychczas skalę**. Wraz z upowszechnieniem się tej technologii rośnie bowiem ryzyko

[2] „Najnowsze narracje dezinformacyjne w polskiej infosferze związane z dronami”, https://www.gov.pl/web/cyfryzacja/najnowsze-narracje-dezinformacyjne-w-polskiej-infosferze-zwiazane-z-dronami (dostęp 13.09.2025 r.).

[3] 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”.

wykorzystywania jej do działań niezgodnych z prawem i etyką. Stanowić to może poważne zagrożenie dla prywatności i bezpieczeństwa jednostek, grup i całych społeczeństw.

Do zagrożeń tych należą zwłaszcza:

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 wyłudzania 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.
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 (np. zmyślone wspomnienia świadków lub zmienione za pomocą technologii nagrania wskazujące na agresję jednego z rodziców).
7. **Zagrożenia dla bezpieczeństwa organizacji.** Deepfake może być wykorzystywany do omijania systemów bezpieczeństwa, takich jak systemy uwierzytelniania biometrycznego, co umożliwia cyberprzestępcom dostęp do danych i systemów podmiotów publicznych i prywatnych, w tym pozyskiwania tajemnic prawnie chronionych.
8. **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.
9. **Naruszenia autorskich praw osobistych** (np. do integralności utworu).

Prezes UODO w swojej praktyce coraz częściej spotyka się przypadkami zrealizowania się niektórych z powyższych zagrożeń.

Przykładem może być 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. Deepfake'owa informacja używała prawdziwych, aktualnych danych osobowych tej osoby. Skarżąca twierdziła, że wykryła aż 263 różne wpisy, których liczba stale rosła. Wskazywała też, że tego rodzaju informacje silnie oddziałują na poczucie jej bezpieczeństwa, godności, prywatności, a także wpływają bardzo negatywnie na stan emocjonalny osób jej bliskich.

W komunikacie dotyczącym tej sprawy Prezes UODO wskazał, że „Osoby publicznie rozpoznawalne, których prawdziwe dane są łatwo dostępne, mogą zostać w sposób okrutny wykorzystane przez cyberprzestępców. Bezprawne użycie danych osobowych i wizerunku może być szczególnie dotkliwe w skutkach nie tylko dla tych osób, ale znacznie szerszego grona zainteresowanych". W tej sprawie organ nadzorczy, uznając, że zaistniała pilna potrzeba ochrony prywatności i wolności skarżącej, zdecydował się wydać postanowienie zobowiązujące spółkę Meta Platforms Ireland Limited do wstrzymania wyświetlania na terytorium Rzeczypospolitej Polskiej przez trzy miesiące[4] na Facebooku i Instagramie fałszywych reklam wykorzystujących prawdziwe dane oraz wizerunek dziennikarki[5].

Innym przykładem może być sprawa dotycząca wygenerowania przez uczniów szkoły podstawowej fałszywego zdjęcia nagiej koleżanki oraz zachęcaniu innych osób do jego zamawiania na platformie Instagram. W tej sprawie Prezes UODO zawiadomił Policję o możliwości popełnienia przestępstwa. Sprawcy, w ocenie Prezesa UODO, mogli dopuścić się modyfikowania oraz następczego ujawniania wizerunku małoletniej koleżanki, co może zostać uznane za przetwarzanie danych osobowych w postaci wizerunku tej osoby, w sytuacji, gdy nie jest to dopuszczalne. Co więcej, takie działanie może również zostać określone jako produkowanie, posiadanie oraz rozpowszechnianie treści pornograficznych z udziałem małoletniego (czyli z uczestnictwem rzeczywistej osoby w wieku poniżej lat 18)[6].

Do Prezesa UODO wpłynęły również sygnały dotyczące lekarzy, którzy padli ofiarą oszustów korzystających z technologii deepfake. Ich wizerunki i autorytet zostały wykorzystane w nieprawdziwych reklamach i zmontowanych materiałach wideo, w których medycy rzekomo zachęcali do przyjmowania określonych preparatów. Takie sytuacje, w przypadku osób wykonujących określone zawody zaufania publicznego (np. lekarze), oprócz naruszenia danych osobowych tych osób i wprowadzania w błąd osób oglądających takie reklamy mogą również powodować, że osoby te są uznawane za podejrzane o naruszenie prawa (czy też np. kodeksu etyki lekarskiej) i wszczynane mogą być wobec nich określone postępowania, np. dyscyplinarne.

Nie budzi wątpliwości, iż w takich – jak wyżej opisane – sprawach mamy do czynienia z przetwarzaniem danych osobowych w rozumieniu art. 4 pkt 1 rozporządzenia 2016/679[7], stosownie do którego dane osobowe oznaczają wszelkie informacje o zidentyfikowanej lub możliwej do zidentyfikowania osobie fizycznej („osobie, której dane

[4] Maksymalny prawnie dopuszczalny okres zgodnie z art. 66 ust. 1 rozporządzenia 2016/679.
[5] Komunikat UODO i treść postanowienia dostępna są pod linkiem: https://uodo.gov.pl/pl/138/3266.
[6] Komunikat UODO dot. tej sprawy dostępny jest pod linkiem: https://uodo.gov.pl/pl/138/3727.
[7] 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".

dotyczą”), zaś 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.

Zgodnie z przepisami rozporządzenia 2016/679 na administratorze spoczywa obowiązek przetwarzania danych osobowych z zachowaniem przesłanek legalizujących wymienionych w art. 6 ust. 1 i art. 9 ust. 2, a ponadto z zachowaniem zasad przetwarzania określonych w art. 5 ust. 1 tego rozporządzenia, w szczególności z zasadą zgodności z prawem, rzetelności i przejrzystości (art. 5 ust. 1 lit. a), a także z zasadą prawidłowości (art. 5 ust. 1 lit. d).

Przetwarzanie, w tym upublicznianie, danych osobowych w postaci deepfake’ów bez podstawy prawnej stanowi naruszenie ww. przepisów dotyczących ochrony danych osobowych.

W ocenie Prezesa UODO ochrona prywatności i bezpieczeństwa w dobie deepfake’ów wymaga kompleksowych działań na poziomie:

1) technologicznym (m.in. wspieranie rozwoju narzędzi weryfikacji autentyczności treści),
2) prawnym (wdrożenie przepisów prawa dotyczących szkodliwego wykorzystania technologii deepfake dostosowanych do szybko zmieniającej się rzeczywistości technologicznej, w tym skutecznych środków ochrony praw osobistych jako niezbywalnych praw jednostki w zakresie jej integralności fizycznej i psychicznej, a także godności i pozycji w społeczeństwie, w tym prawa do ochrony danych osobowych),
3) edukacyjnym (budowanie świadomości i kompetencji, dotyczących zagrożeń związanych z deepfake’mi, sposobów rozpoznawanie fałszywych treści i tego, jak się przed nimi bronić).

Podobnie do tego zagadnienia odnosi się NASK, który dodatkowo wskazuje, że jednym z obszarów przeciwdziałania ww. zagrożeniom jest w jego ocenie również wsparcie ofiar cyberprzestępstw opartych na deepfake’ach poprzez stworzenie specjalnych programów pomocy psychologicznej[8].

Na poziomie prawnym zjawisko deepfake’ów stanowi poważne wyzwanie dla prawodawcy. 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, a jednocześnie często wymykają się tradycyjnym klasyfikacjom prawnym.

W ocenie Prezesa UODO skuteczna walka z tego typu zagrożeniami wymaga dostosowania przepisów do specyfiki technologii deepfake oraz ścisłej współpracy

[8] Materiał pt. „Jak przeciwdziałać zagrożeniom spowodowanym przez deepfaki?” dostępny pod linkiem: https://nask.pl/magazyn/deepfaki-prawdziwy-problem-z-falszywa-rzeczywistoscia.

organów odpowiedzialnych za prawodawstwo oraz nadzór nad sztuczną inteligencją zarówno na poziomie krajowym, jak i międzynarodowym.

Ważne jest uregulowanie kwestii odpowiedzialności za tworzenie i rozpowszechnianie fałszywych treści. **Brak szczegółowych przepisów odnoszących się wprost do deepfake'ów utrudnia ściganie sprawców i skuteczne dochodzenie praw przez ofiary**. Osoby, których dane osobowe (np. wizerunek) zostały wykorzystane w fałszywych materiałach, powinny mieć możliwość szybkiego i łatwego zgłaszania naruszeń, żądania usunięcia treści oraz uzyskania zadośćuczynienia za poniesione szkody.

Jednocześnie zauważyć można, że skuteczne przeciwdziałanie negatywnym skutkom ww. technologii wymaga zaangażowania i współpracy wszystkich uczestników ekosystemu informacyjnego. Dlatego **rozważyć należy również zobowiązanie platform technologicznych/internetowych/społecznościowych do instalowania systemów automatycznego i skutecznego wykrywania oraz oznaczania deepfake'ów.**

Warto również podkreślać i promować **rolę samoregulacji** oraz inicjatyw oddolnych w zwalczaniu zagrożeń związanych z deepfake'ami, zwłaszcza przez branżę technologiczną i medialną. Działania takie mogłyby polegać na wypracowaniu przez nie, a następnie rozwijaniu (na bazie powiększającego się doświadczenia) standardów oraz dobrych praktyk w zakresie weryfikacji autentyczności treści, oznaczania fałszywych materiałów czy reagowania na zgłoszenia użytkowników. W związku z tym można by rozważyć wprowadzenie w krajowym systemie prawa rozwiązań podobnych do kodeksów postępowania, przewidzianych w rozporządzeniu 2016/679.

Odnosząc się do kwestii obowiązujących w Polsce regulacji prawnych dotyczących deepfake'ów zauważyć należy, że przepisy prawa częściowo chronią przed deepfake'ami, choć niedostatecznie i nie wprost, bo nie odnoszą się one bezpośrednio do specyfiki tej technologii.

Art. 81 ustawy o prawie autorskim i prawach pokrewnych[9] wymaga zgody na rozpowszechnianie wizerunku, art. 23 i 24 Kodeksu cywilnego[10] reguluje ochronę dóbr osobistych, w tym wizerunku i głosu, rozporządzenie 2016/679 traktuje wizerunek jako dane osobowe wymagające ochrony. Na podstawie Kodeksu karnego[11] 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).

Z kolei akt w sprawie sztucznej inteligencji wprowadził w art. 50 ust. 4 wymóg oznaczania treści deepfake jako „sztucznie generowane lub zmanipulowane"[12].

---

[9] Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych (Dz.U z 2025 r. poz. 24 ze zm.), dalej jako „prawo autorskie".

[10] Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny (Dz. U. z 2024 r. poz. 1061 ze zm.).

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

[12] Art. 50 ust. 4 aktu w sprawie sztucznej inteligencji: Podmioty stosujące system AI, który generuje obrazy, treści audio lub wideo stanowiące treści deepfake lub który manipuluje takimi obrazami lub treściami, ujawniają, że treści te zostały sztucznie wygenerowane lub zmanipulowane. Obowiązek ten nie ma zastosowania, w przypadku gdy wykorzystywanie jest dozwolone na mocy prawa w celu wykrywania

Ze względu na gwałtownie rosnące możliwości technologii deepfake oraz związane z tym zagrożenia dotyczące nie tylko pojedynczych osób, ale również grup osób, społeczeństwa czy państwa, obecne regulacje nie są jednak dostosowane do specyfiki treści generowanych przez sztuczną inteligencję i możliwości jej negatywnego odziaływania na ludzi. Przede wszystkim żadna z wymienionych wyżej regulacji prawnych nie zapewnia narzędzi do pełnej i skutecznej ochrony przed skutkami takich nadużyć, np. poprzez szybkie usuwanie nielegalnych materiałów. Tymczasem skutki tych nadużyć we współczesnym świecie zdominowanym przez Internet i media społecznościowe są niezwykle dotkliwe, identyfikowanie twórców deepfake'ów często bardzo utrudnione, a procedury sądowe trwają zbyt długo.

W doktrynie podnosi się, że „rozwój technologii deep fake doprowadził do rozdźwięku między stopniem społecznej szkodliwości produkowania, przechowywania i posiadania syntetycznych treści o charakterze pedofilskim z jednej strony oraz ich prezentowania i rozpowszechniania – z drugiej (…). Rodzi to uzasadnioną potrzebę zweryfikowania zasadności różnicowania penalizacji udostępniania prawdziwych treści pornograficznych z udziałem małoletnich oraz tych wytworzonych w formie deep fakes, a przez to potencjalnej nowelizacji art. 202 § 4b k.k. w celu uwzględnienia rozwoju technologicznego, bądź też przeniesienia kwalifikacji prawnej czynów popełnionych z wykorzystaniem deep fakes do art. 202 § 3 k.k. lub innej regulacji typizującej odrębne przestępstwo"[13].

Brak przepisów na poziomie unijnym utrudnia walkę z nadużyciami – dotychczas Unia Europejska nie wprowadziła jednolitych regulacji dotyczących środków ochrony prawnej przed szkodliwymi deepfake'ami, co utrudnia ściganie ich autorów i egzekwowanie odpowiedzialności.

Wobec tego państwa członkowskie we własnym zakresie podejmują próby dostosowywania prawa do szybko zmieniającej się rzeczywistości technologicznej. Przykładem może być Dania, której rząd przygotowuje projekt zmiany prawa autorskiego. Zmienione przepisy mają zapewnić Duńczykom konkretne narzędzia do walki z deepfake'ami. Obywatele będą mogli żądać usunięcia deepfake'ów z platform online oraz dochodzić odszkodowania za naruszenia. Przepisy obejmować mają także „realistyczne, cyfrowo generowane imitacje" występów artystycznych bez zgody. Projekt przewiduje też zachowanie wyjątków dla parodii i satyry, które pozostaną legalne. Celem planowanej regulacji ma być bowiem ochrona obywateli przed złośliwym wykorzystaniem ich wizerunku, a nie ograniczenie wolności wypowiedzi.

Ponadto z informacji zebranych przez Prezesa UODO od innych organów nadzorczych wynika, że w maju tego roku przyjęte zostały przez parlament duński

---

przestępstw, zapobiegania im, prowadzenia postępowań przygotowawczych w ich sprawie lub ścigania ich sprawców. W przypadku gdy treść stanowi część pracy lub programu o wyraźnie artystycznym, twórczym, satyrycznym, fikcyjnym lub analogicznym charakterze obowiązki w zakresie przejrzystości określone w niniejszym ustępie ograniczają się do ujawnienia istnienia takich wygenerowanych lub zmanipulowanych treści w odpowiedni sposób, który nie utrudnia wyświetlania lub korzystania z utworu.

[13] M. Łabuz, M. Małecki, K. Mika-Łabuz, Dziecięca pornografia w formie deep fakes – problemy wykładni na gruncie polskiego prawa karnego i propozycje legislacyjne (Prawo w Działaniu 2025/61/54-84, System Informacji Prawnej LEX, https://sip.lex.pl/komentarze-i-publikacje/czasopisma/dziecieca-pornografia-w-formie-deep-fakes-problemy-wykladni-na-151520848)

przepisy wprowadzające **zakaz deepfake'ów przedstawiających prawdziwe osoby w kontekstach seksualnych.** Zakaz deepfake'ów o takim charakterze został wprowadzony poprawkami do § 226 oraz § 264e duńskiego kodeksu karnego.

Z kolei z informacji przekazanych przez belgijski organ nadzorczy wynika, że w marcu 2023 roku senat belgijski przyjął rezolucję zawierającą stanowiska oraz rekomendacje skierowane do administracji federalnej i terenowej dotyczące kluczowych zagadnień dla problemu deepfake'ów. Jak podkreśla belgijski organ nadzorczy, chociaż rezolucja nie jest prawnie wiążąca, może stanowić podwaliny przyszłych rozwiązań legislacyjnych.

Niderlandzki organ nadzorczy poinformował Prezesa UODO, że chociaż w Niderlandach nie ma obecnie legislacji skierowanej bezpośrednio przeciw deepfake'om, to jego zdaniem zastosowanie mają przepisy niderlandzkiego kodeksu karnego. Wzmocnienia wymaga jednak skuteczność w stosowaniu tego prawa.

Z kolei organ francuski w swojej odpowiedzi wskazał na nowo powstałe ramy regulacyjne dedykowane deepfake'om. Mimo, iż wcześniej nadużycia spowodowane deepfake'ami mogły podlegać przepisom francuskiego kodeksu karnego, m.in. przepisom dotyczącymi kradzieży tożsamości oraz przepisom prawa cywilnego w zakresie prawa do życia prywatnego, to w odpowiedzi na rosnące ryzyko przyjęto nowe szczegółowe przepisy dotyczące deepfake'ów, w tym:

- ustawę dotyczącą wpływów handlowych i zwalczania nadużyć ze strony influencerów w mediach społecznościowych (ustawa nr 2023-451 z 9 czerwca 2023 r.). Art. 5 tej ustawy nakłada na influencerów szczególny obowiązek ujawniania stosowania deepfake'ów, jeśli treść została stworzona przy użyciu sztucznej inteligencji (influencer musi umieścić etykietę: „Wirtualne obrazy"),
- ustawę mającą na celu zabezpieczenie i uregulowanie przestrzeni cyfrowej, która ustanowiła przestępstwo polegające na użyciu deepfake'ów (ustawa nr 2024-449 z 21 maja 2024 r., art. 226-8 i art. 226-8-1 kodeksu karnego).

Warty uwagi kierunek legislacyjnych rozwiązań w odniesieniu do nadużyć związanych z nieautoryzowanymi deepfake'ami wskazuje również amerykańska regulacja, tzw. TAKE IT DOWN Act, Tools to Address Known Exploitation by Immobilizing Technological Deepfakes on Websites and Networks. Zawiera ona definicję cyfrowego fałszerstwa (*digital forgery*). W regulacji tej przewidziano dla platform internetowych obowiązek usuwania zgłoszonych treści w ciągu 48 godzin od zgłoszenia przez ofiarę oraz podejmowania działania w celu usunięcia duplikatów.

Podsumowując, **w ocenie Prezesa UODO w polskim porządku prawnym niezbędne jest wprowadzenie przepisów prawa, które będą bezpośrednio odnosić się do rozpowszechniania szkodliwych treści w postaci deepfake'ów, zapewniając ofiarom możliwość skutecznego i szybkiego dochodzenia ochrony swoich praw**. Przeciwdziałanie specyficznym zagrożeniom powodowanym przez deepfake'i wymaga opracowania szczegółowych zasad ponoszenia odpowiedzialności karnej i odszkodowawczej osób tworzących i rozpowszechniających szkodliwe deepfake'i, a

także doprecyzowania obowiązków podmiotów administrujących platformami internetowymi.

Ponieważ opisywany problem może prowadzić do różnych zagrożeń i naruszeń, w tym dla zdrowia, a nawet życia ludzkiego, tożsamości, danych osobowych, dóbr osobistych oraz demokracji i bezpieczeństwa publicznego, uzasadniona byłaby współpraca różnych sektorów i środowisk oraz ustalenie wspólnej strategii przeciwdziałania zagrożeniom, tak aby ograniczyć skalę i dotkliwość problemu. Nadużywanie tej technologii stanowi poważne zagrożenie dla praw jednostki, demokracji oraz bezpieczeństwa i zaufania publicznego. Obecne ramy prawne Unii Europejskiej, w tym akt w sprawie sztucznej inteligencji, oraz przepisy krajowe, takie jak Kodeks cywilny, Kodeks karny czy prawo autorskie zapewniają jedynie wybiórczą i niewystarczającą odpowiedź na wielopłaszczyznowe zagrożenia związane z deepfake'ami.

W związku z powyższym **zwracam się do Pana Premiera z uprzejmą prośbą o zainicjowanie prac, których celem będzie wprowadzenie w polskim porządku prawnym przepisów, które będą regulować odpowiedzialność prawną za rozpowszechnianie fałszywych treści w postaci deepfake'ów, a także zapewnią skuteczną ochronę danych osobowych.**

Jednocześnie Urząd Ochrony Danych Osobowych oferuje wsparcie eksperckie w ocenie zgodności przyjmowanych w tym zakresie regulacji z przepisami prawa dotyczącymi ochrony danych osobowych.

Uprzejmie proszę Pana Premiera, na podstawie art. 52 ust. 3 ustawy o ochronie danych osobowych, o udzielenie odpowiedzi w terminie 30 dni od daty otrzymania niniejszego wystąpienia.

Łączę wyrazy szacunku

Mirosław Wróblewski
Prezes Urzędu
Ochrony Danych Osobowych