



Ministerstwo Sprawiedliwości

Sekretarz Stanu
Arkadiusz Myrcha

BK-VII.0520.50.2026
Warszawa, 29 kwietnia 2026 r.

Pan
Włodzimierz Czarzasty
Marszałek Sejmu
Rzeczypospolitej Polskiej

Szanowny Panie Marszałku,

w odpowiedzi na interpelację nr 15060 w sprawie aplikacji typu "deepnude" oraz potrzeby wprowadzenia zakazu ich tworzenia, udostępniania i używania w Polsce przedstawiam poniższe stanowisko - w zakresie pytań dotyczących właściwości Ministra Sprawiedliwości.

Ad 1

Ministerstwo Sprawiedliwości nie dysponuje danymi dotyczącymi liczby postępowań karnych i cywilnych prowadzonych w związku z generowaniem i rozpowszechnianiem fałszywych treści intymnych. Z uwagi na konstrukcję systemów sprawozdawczych organów ścigania i wymiaru sprawiedliwości czyny te są obecnie kwalifikowane w oparciu o ogólne przepisy Kodeksu karnego (m.in. art. 190a § 2 czy art. 202), co oznacza, że w statystykach figurują pod tymi jednostkami redakcyjnymi bez wyodrębnienia konkretnego narzędzia technicznego (np. *deepfake*).

Ad 2

Komisja Kodyfikacyjna Prawa Karnego (dalej jako: „KKPK”) przygotowuje opinię, czy obecne przepisy prawnokarne w wystarczający sposób penalizują kwestie rozpowszechniania *deepfake*’ów przy użyciu sztucznej inteligencji (np. poprzez art. 190a

§ 2-3, art. 202 § 4b k.k.¹) i czy niezbędne jest spenalizowanie nowego typu przestępstwa².

Analizowane są również kwestie penalizacji tego przestępstwa w innych państwach Unii Europejskiej³. Do tej pory uzyskano informację dotyczące ustawodawstwa francuskiego (najszerszy model ochrony), niemieckiego (trwają analizy dotyczące wdrożenia przepisów w postulowanym kierunku), słoweńskiego, irlandzkiego, rumuńskiego oraz hiszpańskiego.

Dodatkowo 26 marca 2026 r. Minister Sprawiedliwości powołał Zespół do spraw bezpieczeństwa dzieci i młodzieży w świecie cyfrowym, którego zadaniem jest przygotowanie propozycji regulacji w zakresie zwalczania naruszeń praw dzieci i młodzieży na skutek wytwarzania i rozpowszechniania treści wyprodukowanych z wykorzystaniem sztucznej inteligencji⁴.

Na gruncie prawa cywilnego aktualnie obowiązujące przepisy w pewnym zakresie zapewniają ochronę przed skutkami użycia aplikacji *deepnude*. Używanie aplikacji opartych na sztucznej inteligencji, umożliwiających generowanie realistycznych, fałszywych wizerunków nagich osób na podstawie ich zdjęć może skutkować naruszeniem dóbr osobistych osoby, której zdjęcia zostały w ten sposób użyte. Zgodnie z treścią art. 23 k.c.⁵ wizerunek jest jednym z dóbr osobistych człowieka podlegającym ochronie prawnej. W przypadku wykorzystania tak wytworzonego obrazu w przestrzeni publicznej lub jego udostępnienia osobom trzecim, naruszone zostają inne dobra osobiste (w szczególności cześć, wolność, prawo do prywatności).

Zgodnie natomiast z treścią art. 24 § 1 k.c. *„ten, czyje dobro osobiste zostaje zagrożone cudzym działaniem, może żądać zaniechania tego działania, chyba że nie jest ono bezprawne. W razie dokonanego naruszenia może on także żądać, ażeby osoba, która dopuściła się naruszenia, dopełniła czynności potrzebnych do usunięcia jego skutków,*

¹ ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383; dalej jako: „k.k.”).

² w doktrynie prawnokarnej wskazuje się, że „obowiązujące przepisy wydają się zdadne do ich zaadaptowania do specyfiki *deep fakes* bez konieczności zmian legislacyjnych” - M. Łabuz, M. Małecki, K. Mika-Łabuz, Dziecięca pornografia w formie deep fakes – problemy wykładni na gruncie polskiego prawa karnego i propozycje legislacyjne w: *Prawo w działaniu*, 61/2025, s. 78 (akapit drugi od góry strony).

³ w tym zakresie uruchomiono zapytanie w ramach sieci Legicoop.

⁴ <https://www.gov.pl/web/sprawiedliwosc/du-26-085>

⁵ ustawa z dnia 23 kwietnia 1964 r. - Kodeks cywilny (Dz. U. z 2025 r. poz. 1071 ze zm., dalej: k.c.)

w szczególności ażeby złożyła oświadczenie odpowiedniej treści i w odpowiedniej formie. Na zasadach przewidzianych w kodeksie może on również żądać zadośćuczynienia pieniężnego albo zapłaty odpowiedniej sumy pieniężnej na wskazany cel społeczny.” Tym samym w zakresie odpowiedzialności z tytułu naruszania dóbr osobistych należy przyjąć koncepcję ochrony za pomocą praw podmiotowych bezwzględnych, opartą na założeniu o istnieniu (wyrażonego w art. 23 k.c.) powszechnego zakazu naruszania dóbr osobistych innych osób. Każde naruszenie dobra osobistego jest bezprawne *per se*, ponieważ narusza ten ustawowy i generalny zakaz⁶.

Wskazać także należy, że działająca przy Ministrze Sprawiedliwości Komisja Kodyfikacyjna Prawa Cywilnego dostrzegła konieczność całościowego spojrzenia na regulacje odnoszące się do ochrony dóbr osobistych, odpowiedniej równowagi i proporcji pomiędzy środkami ochrony dóbr osobistych oraz wolności słowa, a także na konieczność pilnego uwzględnienia konsekwencji wynikających z rozwoju nowych technologii informatycznych, sztucznej inteligencji i coraz bardziej poszerzającej się skali różnorodnych wcześniej nieznanymi środkami naruszania dóbr osobistych. Podjęte zostały wstępne działania zmierzające do opracowania założeń rozwiązań służących ochronie dóbr osobistych i wolności słowa - w obszarze prawa cywilnego. Planowane są również wspólne działania Komisji Kodyfikacyjnej Prawa Cywilnego i Komisji Kodyfikacyjnej Prawa Karnego. Efekt prac Komisji Kodyfikacyjnej Prawa Cywilnego dostępny jest na stronie internetowej Ministerstwa Sprawiedliwości w zakładce dedykowanej pracom Komisji⁷.

Ad 3

Kwestia ewentualnego wprowadzenia ustawowego zakazu tworzenia i udostępniania konkretnych typów oprogramowania (np. aplikacji typu *deepnude*) jest obecnie przedmiotem pogłębionej analizy prawnej oraz technicznej. Należy wskazać, że skuteczność tego rodzaju zakazów krajowych musi być rozpatrywana w kontekście przepisów unijnych (w szczególności Aktu o Sztucznej Inteligencji – AI Act) oraz transgranicznego charakteru usług cyfrowych. W tym kontekście istotne są prace

⁶ P. Machnikowski, w: *Kodeks cywilny. Komentarz*, red. E. Gniewek, P. Machnikowski, Legalis/el. 2023, komentarz do art. 24, nb. 5.

⁷ <https://www.gov.pl/web/sprawiedliwosc/projekty-aktow-prawnych3>

wspomnianego Zespołu ds. bezpieczeństwa dzieci oraz opinia KKPK, która ma wskazać, czy obecne instrumenty prawnokarne (m.in. w zakresie zwalczania pornografii bez zgody) są wystarczające, czy też wymagają penalizacji samego etapu wytwarzania narzędzi służących do popełniania tych czynów.

Ad 4

Pytanie dotyczy właściwości Ministra Cyfryzacji. Należy jednak wskazać, że ustawa wdrażająca tzw. DSA – Digital Services Act, czyli unijne rozporządzenie o usługach cyfrowych z dnia 19 października 2022 r. (której przepisy w UE weszły w życie 17 lutego 2024 r.), zwiększająca ochronę użytkowników Internetu przed nielegalnymi treściami, 9 stycznia 2026 r. została zawetowana przez Prezydenta.

Ad 5

Ministerstwo Sprawiedliwości dostrzega potrzebę usprawnienia procedur „takedown” (szybkiego usuwania treści). W obszarze wsparcia osób pokrzywdzonych kluczową rolę odgrywa Sieć Pomocy Osobom Pokrzywdzonym Przystępstwem (finansowana z Funduszu Sprawiedliwości), która zapewnia bezpłatną pomoc prawną, psychologiczną oraz materialną. Jednocześnie skuteczność mechanizmów szybkiego usuwania treści jest ściśle skorelowana z wdrożeniem unijnych regulacji o usługach cyfrowych, o których mowa w pkt 4.

Ad 6

Pytanie dotyczy aktów prawnych takich jak *Digital Services Act (DSA)* oraz *Aktu o Sztucznej Inteligencji (AI ACT)* będących w właściwości Ministra Cyfryzacji.

Jednocześnie wskazuję, że Ministerstwo Sprawiedliwości opracowało „Wytyczne do standardów ochrony dzieci - ochrona dziecka w Internecie”. Standardy ochrony małoletnich są jednym z instrumentów wprowadzonych przez ustawę z 13 maja 2026 r. o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich⁸ (dalej ustawa o ochronie małoletnich). Stanowią one zbiór zasad i reguł

⁸ t.j. Dz.U. z 2024 r. poz. 1802

mających na celu zapewnienie bezpieczeństwa dzieci oraz ochronę przed wszelkimi formami krzywdzenia, wykorzystywania i zaniedbywania.

W ww. wytycznych Ministerstwo Sprawiedliwości radzi, w jaki sposób podmioty zobowiązane do wprowadzenia standardów ochrony małoletnich mogą opisać rodzaje zagrożeń, które związane są z Internetem i nowymi technologiami, dodatkowe zasady interwencji w przypadku wystąpienia takich zdarzeń, rolę i zadania koordynatora bezpieczeństwa w sieci, zabezpieczenia sieci i urządzeń, wskazują działania edukacyjne związane z bezpieczeństwem w Internecie. Materiały te są dostępne pod adresem <https://www.gov.pl/web/sprawiedliwosc/wytyczne-do-standardow-ochrony-dzieci---ochrona-dziecka-w-internecie>

Dodatkowo wyjaśniam, że Ministerstwo Sprawiedliwości przygotowuje projekt ustawy o zmianie ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich. Przewidziano w nim m. in. rozwiązania, które podkreślają znaczenie ochrony wizerunku małoletniego. Przepisy dotyczące ochrony wizerunku małoletniego - art. 22zd - 22zf – zamieszczone są w rozdziale dotyczącym ochrony danych osobowych. Mają one na celu wprowadzenie do ustawy kompleksowej regulacji dotyczącej ochrony wizerunku małoletnich, uwzględniającej zarówno standardy wynikające z rozporządzenia 2016/679 (RODO), jak i specyficzne ryzyka wskazywane przez organ nadzorczy – Prezesa Urzędu Ochrony Danych Osobowych – w odniesieniu do przetwarzania wizerunku dzieci, w szczególności w środowisku cyfrowym. Wizerunek małoletniego stanowi daną osobową w rozumieniu RODO, co potwierdza zarówno ugruntowana praktyka, jak i stanowisko Prezesa UODO. Jednocześnie RODO podkreśla konieczność szczególnej ochrony danych dzieci, które są mniej świadome ryzyk związanych z ich przetwarzaniem i wymagają zwiększonego poziomu gwarancji.

W aktualnym stanie prawnym zasady przetwarzania wizerunku dzieci wynikają jedynie pośrednio z przepisów RODO, co prowadzi w praktyce do niejednolitego, często niewystarczającego poziomu ochrony. Jednocześnie z dokumentów i analiz dotyczących wykorzystywania zdjęć dzieci w sieci – w tym materiałów edukacyjnych UODO i raportów dotyczących cyberzagrożeń – wynika, że małoletni są szczególnie narażeni na bezprawne

wykorzystanie ich wizerunku (deepfake, fotomontaże, wtórne rozpowszechnianie, przemoc rówieśnicza, wykorzystywanie przez osoby o skłonnościach pedofilskich).

Wobec tych zagrożeń przepisy ustawy nowelizującej w art. 22zd-22zf: precyzują obowiązek uzyskania zgody przedstawiciela ustawowego lub małoletniego powyżej 16 roku życia, zgodnie z zasadą świadomego, dobrowolnego i konkretnego wyrażenia zgody (art. 6 i 7 RODO), wprowadzają wymogi co do treści zgody – takie jak cel, zakres i sposób publikacji – co umożliwi spełnienie obowiązku informacyjnego i zapewni zgodność przetwarzania z zasadą przejrzystości (art. 5 ust. 1 lit. a RODO), regulują sposób dokumentowania zgód, co odpowiada zasadzie rozliczalności (art. 5 ust. 2 RODO), określają zasady powierzania przetwarzania wizerunku zgodnie z art. 28 RODO, co zapobiega niekontrolowanemu dalszemu rozpowszechnianiu wizerunku małoletniego, wprowadzają zakaz wykorzystywania wizerunku do celów wykraczających poza zakres zgody, co pozostaje w zgodzie z zasadą minimalizacji i ograniczenia celu (art. 5 ust. 1 lit. b i c RODO). Prace prowadzone w Ministerstwie Sprawiedliwości nad ustawą o zmianie ustawy o przeciwdziałaniu zagrożeniom przestępczością na tle seksualnym i ochronie małoletnich, znajdują się na etapie końcowym uzgodnień wewnątrzresortowych.

Z wyrazami szacunku
Arkadiusz Myrcha
Sekretarz Stanu
/podpisano elektronicznie/