Ministerstwo
Cyfryzacji

Sekretarz Stanu
Dariusz Standerski

BM.WP.057.200.2025
Warszawa, 03 stycznia 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 30 października br. Posłanek na Sejm RP Pań Katarzyny Matusik-Lipiec, Elżbiety Anny Polak, Iwony Małgorzaty Krawczyk, Iwony Hartwich, Anny Sobolak, Alicji Łuczak, Magdaleny Łośko w sprawie ochrony osób fizycznych przed nieautoryzowanym wykorzystaniem ich głosu, wizerunku i innych cech osobistych przez systemy sztucznej inteligencji (interpelacja nr 13153)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłanki pytania.

Ad 1) Czy ministerstwo prowadzi obecnie prace nad opracowaniem krajowych regulacji prawnych dotyczących ochrony osób fizycznych przed nieautoryzowanym wykorzystaniem ich głosu, wizerunku lub innych cech osobistych przez systemy sztucznej inteligencji?

Ochrona osób fizycznych przed nieautoryzowanym wykorzystaniem ich głosu, wizerunku lub innych cech osobistych przez systemy sztucznej inteligencji kształtuje się w oparciu o przepisy rozporządzenia 2024/1689 AI Act, z naciskiem na art. 50 dot. obowiązków informacyjnych, które obecnie wynikają wprost z rozporządzenia. Rozporządzenie jest częścią polskiego porządku prawnego i bezpośrednio oddziałuje na rzeczywistość prawną państw członkowskich. Wspomagające do rozporządzenia będą przepisy rozporządzenia o danych osobowych (RODO) dot. danych osobowych powstałych w wyniku specjalnego przetwarzania technicznego, dot. cech fizycznych, fizjologicznych lub behawioralnych osoby fizycznej.

Ministerstwo Cyfryzacji prowadzi równolegle prace nad projektem ustawy o systemach sztucznej inteligencji (numer z wykazu RCL: UC71), który na obecnym etapie uwzględnia m.in.:

- ustanowienie krajowego organu nadzoru rynku odpowiedzialnego za egzekwowanie przepisów rozporządzenia 2024/1689 (AI Act);
- procedury kontroli i postępowania administracyjnego w przypadku naruszenia przepisów rozporządzenia, w tym nielegalnego przetwarzania danych biometrycznych;
- możliwość nakładania administracyjnych kar pieniężnych za stosowanie systemów AI niezgodnych z prawem, w tym tych, które naruszają prawa podstawowe osób fizycznych.

Planowane w najbliższych miesiącach wejście w życie projektu ustawy istotnie zwiększy możliwość nadzoru nad systemami sztucznej inteligencji w Polsce, w tym ochrony obywateli przed nieuprawnionym wykorzystaniem ich cech osobistych przez takie systemy.

Ad 2) Czy planowane są działania legislacyjne mające na celu uzupełnienie obowiązującego prawa cywilnego, karnego lub autorskiego o przepisy odnoszące się wprost do generatywnej AI i zjawiska deepfake?

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Ze względu na właściwość tematyczną pytania Ministerstwo Cyfryzacji zwróciło się do Ministerstwa Sprawiedliwości, jak i Ministerstwa Kultury i Dziedzictwa Kulturowego z prośbą przekazanie wkładu do odpowiedzi.

W pierwszej kolejności należy wspomnieć o projekcie ustawy o systemach sztucznej inteligencji (UC71) , który przygotowało Ministerstwo Cyfryzacji. Projekt służy stosowaniu w krajowym porządku prawnym rozporządzenia 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.

Ww. rozporządzenie Parlamentu Europejskiego i Rady, mające bezpośrednie zastosowanie w Polsce i częściowo obowiązujące od 2 lutego 2025 roku (Rozdział I: Przepisy Ogólne oraz Rozdział II: Zakazane Praktyki) oraz od 2 sierpnia 2025 roku (Rozdział III: Systemy AI Wysokiego Ryzyka: Sekcja 4: Organy Notyfikujące i Jednostki Notyfikowane; Rozdział V: Modele AI Ogólnego Przeznaczenia; Rozdział VII: Zarządzanie; Rozdział XII: Kary oraz art. 78 z wyjątkiem art. 101), definiuje deepfake jako 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 (art. 3 pkt 60 ww. rozporządzenia). Do zjawiska deepfake odnosi się również art. 50 ust. 4 ww. rozporządzenia, który będzie mógł być stosowany bezpośrednio od 2 sierpnia 2026 r.

Ochrona na gruncie prawa cywilnego

Problematyka związana z ochroną osób fizycznych przed nieautoryzowanym wykorzystaniem ich głosu, wizerunku i innych cech osobistych przez systemy sztucznej inteligencji, wpisuje się w szerzy problem związany z nadużyciami w Internecie.

Na gruncie prawa cywilnego takie zjawiska można rozpatrywać w kontekście naruszeń dóbr osobistych. Dobra osobiste nie posiadają legalnej definicji. W art. 23 ustawy z dnia 23 kwietnia 1964 r. – Kodeks cywilny ustawodawca poprzestał na egzemplifikacji wybranych dóbr (tj. zdrowia, wolności, czci, swobody sumienia, nazwiska lub pseudonimu, wizerunku, tajemnicy korespondencji, nietykalności mieszkania, twórczości naukowej, artystycznej, wynalazczej i racjonalizatorskiej) oraz na potwierdzeniu pozostawania wszystkich dóbr osobistych człowieka pod ochroną prawa cywilnego, niezależnie od ochrony przewidzianej w innych przepisach. Tym samym na przedstawicielach doktryny i judykatury spoczywa zadanie stwierdzania istnienia kolejnych dóbr osobistych, innych niż wymienione przykładowo w art. 23 k.c. Nie budzi wątpliwości, że dobrem osobistym istniejącym a niewskazanym w tym przepisie jest życie – podstawowe dobro osobiste człowieka, pozwalające na korzystanie z innych dóbr.

Istnieją także dobra osobiste odkodowane w związku z kształtowaniem się nowych stosunków społecznych i potrzebą ochrony wartości i interesów człowieka[1]. W tym kontekście nie można wykluczyć, by wobec znacznej aktywności internetowej, w tym także zjawisk niepożądanych, a występujących wyłącznie w przestrzeni wirtualnej, pojawiła się kolejna kategoria dóbr osobistych, związanych wyłącznie z ochroną jednostki w Internecie.

Ministerstwo Sprawiedliwości nie prowadzi aktualnie prac zmierzających do uzupełnienia obowiązującego prawa cywilnego o przepisy odnoszące się wprost do zjawisk

[1] B. Janiszewska, [w:] Kodeks cywilny. Komentarz. Tom I. Część ogólna, cz. 1 (art. 1–55(4)), red. J. Gudowski, LEX 2021, komentarz do art. 23, teza 1.

zachodzących w przestrzeni internetowej, w tym treści generatywnych przez AI czy zjawiska deepfake.

Wskazać natomiast 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, w tym w szczególności sztucznej inteligencji i coraz bardziej poszerzającej się skali różnorodnych kompletnie wcześniej nieznanych środków naruszania dóbr osobistych.

Z tych przyczyn zostały podjęte wstępne działania zmierzające do opracowania założeń rozwiązań służących ochronie dóbr osobistych i wolności słowa, w obszarze prawa cywilnego. Zgodnie z planem, w dalszej kolejności, zintensyfikowane zostaną działania Komisji Kodyfikacyjnej Prawa Cywilnego i Komisji Kodyfikacyjnej Prawa Karnego w tym przedmiocie. Intencją Komisji jest wypracowanie rozwiązań o kompleksowym, stanowiących realną i adekwatną odpowiedź na niepożądane zjawiska związane z rozwojem nowych technologii.

Wstępny etap prac uniemożliwia jednak przedstawienie bardziej precyzyjnych założeń i planowanych rozwiązań, w tym także przesądzenie w jakim stopniu projektowane rozwiązania odnosić się będą wprost do omawianego zjawiska. Efekt prac Komisji Kodyfikacyjnej Prawa Cywilnego dostępny jest jednak na stronie internetowej Ministerstwa Sprawiedliwości w zakładce dedykowanej pracom Komisji.

Ochrona na gruncie prawa karnego

W kontekście ogólnej uwagi interpelacji, że „obecne przepisy nie przewidują ani jasnych zasad odpowiedzialności za wykorzystanie czyjegoś głosu lub wizerunku przez modele AI, ani procedur pozwalających na szybkie usuwanie takich treści z Internetu" wyjaśniam, że obowiązuje przepisy prawa karnego materialnego już obecnie właściwie penalizują wymienione w interpelacji przestępstwa w postaci kradzieży tożsamości, oszustwa internetowego czy nieuprawnionego pozyskiwania danych osobowych.

W tym zakresie przywołać należy przede wszystkim:

- przestępstwo kradzieży tożsamości z art. 190a § 2 k.k. (w każdy sposób, także elektronicznie), zagrożone karą pozbawienia wolności do lat 8,
- przestępstwo oszustwa z art. 286 § 1 k.k. (które penalizuje każdy rodzaj oszustwa) i jest zagrożone surową karą do 8 lat pozbawienia wolności,
- przestępstwo oszustwa z art. 287 § 1 k.k. (polegające przede wszystkim na wpływaniu bez upoważnienia na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych w celu osiągnięcia korzyści majątkowej), zagrożone karą pozbawienia wolności do lat 5,
- przestępstwo bezprawnego uzyskania informacji lub dostępu do całości lub części systemu informatycznego (art. 267 § 1 i 2 k.k.), zagrożone karą grzywny, karą ograniczenia wolności albo pozbawienia wolności do lat 2,
- przestępstwo nielegalnego przetwarzania danych osobowych z art. 107 ust. 1 i 2 ustawy o ochronie danych osobowych, które, w zależności od rodzaju nielegalnie przetwarzanych danych, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2, albo grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 3.

W zależności od ustalonego w sprawie stanu faktycznego i wyczerpania przez sprawcę jednym czynem znamion więcej niż jednego przepisu karnego, ww. przestępstwa mogą pozostawać w zbiegu z innymi – np. przestępstwem utrudniania zapoznania się z

informacją (art. 268 k.k.), przestępstwem niszczenia danych informatycznych (art. 268a k.k.), przestępstwem uszkadzania danych informatycznych (art. 269 k.k.), przestępstwem zakłócania systemu komputerowego (art. 269a) i innymi przestępstwami, np. przeciwko wolności, wolności seksualnej i mieniu.

W Ministerstwie Sprawiedliwości w najbliższym czasie nie są planowane zmiany w zakresie prawa karnego materialnego w obszarze objętym interpelacją.

Na podpis Prezydenta RP oczekuje ustawa z dnia 18 grudnia 2025 r. o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw. W zakresie tematyki interpelacji ustawa obejmuje nowe rozwiązania, mające zminimalizować nielegalne treści w Internecie. Ustawa przewiduje mianowicie uprawnienie dla m.in. prokuratora, Policji, KAS-u, Straży Granicznej, w zakresie określonych przestępstw (w tym m.in. art. 189a, 119 § 1, 148a § 1, 190 § 1, 190a § 2, 200 § 3 i 5, 256 § 1 i 2, 286 § 1, 287 § 1 k.k.), do złożenia wniosku o wydanie nakazu podjęcia działań przeciwko nielegalnym treściom polegającego na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich, których rozpowszechnianie może wyczerpywać znamiona czynu zabronionego, a także nawołujących do popełnienia czynu zabronionego. Kryteria, które zostały w ustawie przyjęte przy enumeratywnym odesłaniu do konkretnych czynów zabronionych, są trzy:

- zakwalifikowanie danego przestępstwa jako przestępstwa internetowego rozumianego jako przestępstwo związane z Internetem według sposobu działania (modus operandi) sprawcy,
- przestępstwo internetowe jest związane z rozpowszechnianiem treści,
- uniemożliwienie dostępu do treści nie powoduje negatywnych skutków dla dyskursu obywatelskiego i procesów wyborczych.

Skutkiem przeprowadzonego postępowania może być wg projektu wydanie przez organ właściwy do rozpatrzenia wniosku decyzji zawierającej nakaz uniemożliwienia dostępu do nielegalnych treści. Dodatkowo wskazuję, że przed cyberatakami w pierwszej kolejności chronią mechanizmy wypracowane przez Ministerstwo Cyfryzacji oraz działające w strukturach Policji Centralne Biuro Zwalczania Cyberprzestępczości (zob. art. 5d ustawy o Policji).

Zarówno phishing jak i cyberstalking są w Polsce karane, odpowiednio jako przestępstwo z art. 287 § 1 k.k. i art. 190a § 1 k.k.

W zakresie technologii deepfake wskazuję zaś, że już na gruncie obecnie obowiązujących przepisów sprawca wykorzystujący tę technologię, w zależności od celu jej zastosowania, może ponosić odpowiedzialność m.in. z ustawy o prawie autorskim i prawach pokrewnych, która to ustawa wymaga zgody na rozpowszechnianie wizerunku. Sprawca może też odpowiadać karnie, m.in. z art. 107 ust. 1 i 2 ustawy o ochronie danych osobowych za nielegalne przetwarzanie danych, z art. 190a § 2 k.k. (kradzież tożsamości), z art. 191 k.k. (zmuszanie do określonego zachowania),z art. 191a k.k. (rozpowszechnienie wizerunku nagiej osoby bez zgody), z art. 202 k.k. (publiczna prezentacja lub produkcja, rozpowszechnianie, przechowywanie i posiadanie treści pornograficznych, z art. 212 i 216 k.k. (zniesławienie lub zniewaga) lub z art. 286 k.k. (oszustwo).

Z racji na ważkość omawianego problemu Ministerstwo Sprawiedliwości – Departament Prawa Karnego stale monitoruje otoczenie legislacyjne w tym zakresie oraz informacje przekazywane m.in. przez Prokuraturę Krajową.

Zjawisko deepfake dotyka dóbr osobistych uregulowanych w KC oraz prawa do wizerunku w ustawie o prawie autorskim i prawach pokrewnych.

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Ew. nowelizacja KC nie jest w kompetencji MKiDN. Natomiast gdy chodzi o prawo autorskie, to art. 81 ustawy już teraz gwarantuje prawo do wizerunku stanowiąc, że „rozpowszechnianie wizerunku wymaga zezwolenia osoby na nim przedstawionej". W kontekście deepfake MKiDN prowadzi obecnie analizy, czy jest to regulacja wystarczająca. W szczególności dotyczy to takich kwestii jak konieczność ew. doprecyzowania, że wizerunek obejmuje też głos czy sposób zachowania danej osoby oraz czy konieczne jest wzmocnienie ochrony tak rozumianego wizerunku gwarantowanej prawem cywilnym przez wprowadzenie w określonym zakresie także odpowiedzialności karnej. Analizujemy też działania podejmowane w omawianym obszarze przez pozostałe państwa UE, w szczególności sprawującą obecnie Prezydencję w Radzie UE Danię. Na ten moment jest jeszcze za wcześnie, aby zakomunikować, jakie zmiany zostaną wprowadzone.

Gdy chodzi natomiast o blokowanie stron internetowych rozpowszechniających materiały klasyfikowane jako deepfake kluczowe znaczenie ma przygotowana przez MC i procedowana obecnie w Sejmie nowelizacja uśude.

Ad 3) Jakie mechanizmy egzekucji i ochrony prawnej (np. prawo do usunięcia treści, odpowiedzialność platform, prawo do odszkodowania) są rozważane w ramach wdrażania nowych przepisów w Polsce? Czy Polska zamierza przyjąć rozwiązania inspirowane tzw. modelem duńskim, przyznając obywatelom prawo do ich cyfrowego wizerunku i głosu jako chronionego dobra prawnego?

W polskim porządku prawnym ochrona przed nieautoryzowanym wykorzystaniem wizerunku, głosu czy tożsamości osoby fizycznej opiera się obecnie na przepisach o dobrach osobistych (art. 23–24 kodeksu cywilnego), prawie do wizerunku (art. 81 ustawy o prawie autorskim i prawach pokrewnych), wybranych przepisach prawa karnego (np. zniesławienie, stalking), a także na regulacjach unijnych, w szczególności RODO, DSA i DMA.

W ramach wdrażania nowych przepisów, w tym ustawy o systemach sztucznej inteligencji (UC71), Polska rozwija system ochrony prawnej, który obejmuje:

a) mechanizmy egzekucji i nadzoru - projekt ustawy o AI przewiduje utworzenie krajowego organu nadzoru rynku – Komisji Rozwoju i Bezpieczeństwa Sztucznej Inteligencji – wyposażonej w kompetencje do kontroli, wydawania decyzji, nakładania kar oraz egzekwowania zakazów stosowania systemów AI naruszających prawa podstawowe, w tym prawa do wizerunku i głosu;
b) prawo do usunięcia treści i sprzeciwu – wraz z wejściem w życie Digital Services Act (DSA), użytkownicy zyskują dostęp do procedur „*notice and action*" (ang. zgłoś i działaj), prawa do odwołania od decyzji platformy oraz możliwości złożenia skargi do krajowych organów nadzorczych (UKE, KRRiT). RODO zapewnia dodatkowo prawo do bycia zapomnianym (art. 17), czyli usunięcia danych osobowych, w tym danych biometrycznych, głosu czy wizerunku.
c) odpowiedzialność platform. Projekt ustawy wdrażającej DSA przewiduje odpowiedzialność cywilną, administracyjną i karną dostawców usług cyfrowych za naruszenia przepisów, w tym za nielegalne wykorzystanie danych osobowych i naruszenie dóbr osobistych.
d) w zakresie prawa do odszkodowania istnieją dwa tryby dochodzenia roszczeń - osoby fizyczne mogą dochodzić roszczeń z tytułu naruszenia dóbr osobistych na podstawie kodeksu cywilnego (jw.), a także dochodzić odszkodowania za naruszenie przepisów RODO (art. 82), w przypadku szkody materialnej lub niematerialnej.

Odnosząc się do tzw. modelu duńskiego, który zakłada uznanie cyfrowego wizerunku i głosu za chronione dobra prawne, należy wskazać, że obecnie w Polsce nie funkcjonuje

odrębna regulacja przyznająca obywatelom takie prawo wprost. Niemniej jednak, projekt ustawy o systemach sztucznej inteligencji oraz wskazane wyżej przepisy DSA i RODO tworzą podstawy do budowania interpretacji o uznaniu cyfrowych cech tożsamości (w tym głosu i wizerunku) za elementy podlegające ochronie prawnej – zarówno w kontekście danych osobowych, jak i dóbr osobistych.

Ad 4) Czy ministerstwo planuje kampanie informacyjne lub programy edukacyjne, które podniosłyby świadomość społeczną w zakresie zagrożeń wynikających z rozwoju generatywnej AI oraz możliwości prawnej ochrony jednostki?

Ministerstwo Cyfryzacji dostrzega potrzebę wzmacniania świadomości społecznej w zakresie wyzwań i zagrożeń związanych z rozwojem generatywnej sztucznej inteligencji, w tym w obszarach takich jak ochrona danych osobowych, dezinformacja, naruszenia dóbr osobistych czy profilowanie.

W zaprezentowanym przez Ministra Cyfryzacji projekcie Polityki rozwoju sztucznej inteligencji w Polsce do 2030 r., który obecnie oczekuje na skierowanie do dalszego procedowania legislacyjnego, przewidziano szereg działań edukacyjnych i informacyjnych. Na tym etapie prac uwzględniono m.in.:

- potrzebę realizacji programów edukacyjnych i kampanii informacyjnych dla obywateli, mających na celu zwiększenie kompetencji cyfrowych oraz wiedzy o prawach jednostki w kontekście AI;
- rozwój narzędzi wspierających edukację w zakresie bezpiecznego i etycznego korzystania z technologii AI, w tym generatywnej;
- budowę platformy informacyjnej poświęconej sztucznej inteligencji, która ma służyć jako źródło wiedzy, materiałów edukacyjnych oraz informacji o dostępnych mechanizmach ochrony prawnej.

Wyżej wylistowane działania mają na celu zarówno informowanie o potencjalnych zagrożeniach, ale także wspieranie obywateli w świadomym i bezpiecznym korzystaniu z rozwiązań opartych na sztucznej inteligencji, by wraz z rozwojem świadomości o AI, wzmacniać polskie talenty w tym zakresie.

Ad 5) Czy przewidziano współpracę międzyresortową oraz konsultacje z branżą medialną, środowiskiem twórców internetowych i organizacjami zajmującymi się ochroną praw cyfrowych w celu wypracowania kompleksowych rozwiązań w tym zakresie?

Wyżej wspominany już projekt ustawy o systemach sztucznej inteligencji (UC71) jest procedowany w trybie rządowym, co oznacza, że zgodnie z obowiązującymi zasadami legislacyjnymi przewidziane są konsultacje publiczne i międzyresortowe. Analogicznie, zaprezentowana przez Ministra Cyfryzacji Polityka rozwoju sztucznej inteligencji w Polsce do 2030 roku – dokument strategiczny, który w najbliższym będzie przedmiotem procesu legislacyjnego – również zakłada szerokie konsultacje społeczne i międzysektorowe. W ramach prac nad Polityką AI wskazano również konkretne obszary, które będą realizowane we współpracy z innymi resortami – m.in. w zakresie edukacji, kultury, ochrony zdrowia, sprawiedliwości czy rynku pracy. Dokument ten zakłada podejście horyzontalne, uwzględniające potrzebę współpracy międzysektorowej i międzyinstytucjonalnej, w tym z branżą medialną, środowiskiem twórców internetowych oraz organizacjami zajmującymi się ochroną praw cyfrowych.

Z wyrazami szacunku

Dariusz Standerski
Sekretarz Stanu
/dokument podpisany elektronicznie/

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

telefon +48 22 245 54 42
adres email sekretariat.BM@cyfra.gov.pl
www.gov.pl/web/cyfryzacja

ul. Królewska 27
00-060 Warszawa