Ministerstwo
Cyfryzacji

Sekretarz Stanu
Dariusz Standerski

BM.WP.057.62.2026
Warszawa, 24 maja 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 24 marca br. Posłanki na Sejm RP Pani Olgi Ewy Semeniuk-Patkowskiej w sprawie zagrożeń związanych z wykorzystaniem technologii deepfake (interpelacja nr 16013)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłankę pytania.

Ad 1) Czy instytucje państwowe monitorują skalę wykorzystania technologii deepfake w Polsce?

Ministerstwo analizuje jak znakować treści tworzone przez AI, zwłaszcza w związku z wdrożeniem AI Act. Od 2 sierpnia 2026 r. dostawcy systemów generatywnej AI będą musieli oznaczać treści syntetyczne i ujawniać ich sztuczne pochodzenie (art. 50 AI Act).

Dezinformacja generowana przez AI została wprost wskazana jako jedno z kluczowych wyzwań społecznych w Polityce rozwoju sztucznej inteligencji w Polsce do 2030 r. (Polityka AI), wpisanej do wykazu prac legislacyjnych i programowych Rady Ministrów w dn. 31 marca (ID260). Cel 5 Polityki AI zakłada stworzenie ogólnodostępnego narzędzia do wykrywania dezinformacji AI, a jego realizacja jest planowana do 2030 r.

Ad 2) Ile przypadków wykorzystania materiałów deepfake w działaniach przestępczych odnotowano w latach 2023–2026?

Dane statystyczne dotyczące przestępstw z użyciem deepfake gromadzą organy ścigania. Po szczegółowe informacje należy zwrócić się do Komendy Głównej Policji lub Prokuratury Krajowej.

Ad 3) Czy prowadzone są analizy dotyczące wpływu technologii deepfake na bezpieczeństwo informacyjne państwa?

Ministerstwo Cyfryzacji w ramach swojej właściwości śledzi kwestie przejrzystości systemów AI i dezinformacji cyfrowej w kontekście tworzenia regulacji krajowych i unijnych. Dezinformacja generowana przez AI została wskazana w Polityce AI jako jedno z kluczowych wyzwań społecznych wymagających działań edukacyjnych (zob. odpowiedź na pytanie 1).

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

ul. Królewska 27
00-060 Warszawa

Ad 4) Jakie instytucje państwowe są odpowiedzialne za monitorowanie zagrożeń związanych z wykorzystaniem tej technologii?

Za monitorowanie zagrożeń w cyberprzestrzeni, w tym związanych z treściami generowanymi przez AI, odpowiadają przede wszystkim:

I. CSIRT GOV (ABW) — właściwy dla administracji rządowej;
II. CSIRT NASK (NASK) — właściwy dla operatorów i obywateli;
III. CSIRT MON — właściwy dla podmiotów podległych Ministrowi Obrony Narodowej.

Wszystkie trzy podmioty działają na podstawie ustawy o krajowym systemie cyberbezpieczeństwa. Szczególną rolę odgrywa NASK, który prowadzi Ośrodek Badań nad Bezpieczeństwem Sztucznej Inteligencji, czyli jednostkę zajmującą się wykrywaniem wzorców, generowaniem treści multimedialnych i ochroną modeli AI przed atakami (sekcja 4.4 Polityki AI). Planowane jest dalsze rozwijanie Ośrodka oraz tworzenie podobnych zespołów badawczych w innych krajowych jednostkach B+R.

Ad 5) Czy istnieją procedury pozwalające na identyfikację materiałów deepfake w internecie?

Na poziomie Unii Europejskiej trwają prace nad skoordynowanymi procedurami i standardami technicznymi w tym zakresie. Kluczowym instrumentem prawnym jest art. 50 AI Act, który zobowiąże dostawców systemów generatywnej AI do znakowania treści syntetycznych, do czego docelowo prawdopodobnie będzie stosować się metadane z podpisem cyfrowym i niewidoczne dla ludzkiego oka znaki wodne. Rozwiązania mają na celu udostępnić narzędzia umożliwiające weryfikację pochodzenia treści organom publicznym, badaczom i mediom.

Równolegle opracowywany jest Kodeks Przejrzystości Treści Generowanych przez AI (art. 56 AI Act) – odrębny od Kodeksu Dobrych Praktyk dla modeli ogólnego przeznaczenia (GPAI Code of Practice), którego pierwsza wersja ukazała się w 2025 r.

Polska uczestniczy w pracach nad wdrożeniem tych rozwiązań za pośrednictwem Ministerstwa Cyfryzacji w strukturach Rady UE i AI Board.

Ad 6) Czy Ministerstwo współpracuje w tym zakresie z platformami internetowymi i mediami społecznościowymi?

Duże platformy internetowe sklasyfikowane jako Very Large Online Platforms (VLOPs) podlegają rozporządzeniu o usługach cyfrowych (DSA), które nakłada na nie obowiązki w zakresie zarządzania ryzykiem systemowym, w tym zagrożeniami związanymi z dezinformacją i treściami manipulowanymi. Bezpośredni nadzór nad VLOPs sprawuje Komisja Europejska.

W ramach Polityki AI Ministerstwo uczestniczy ponadto w tworzeniu i opiniowaniu europejskich regulacji dotyczących AI, w tym zasad odpowiedzialności platform za treści generowane przez AI.

Ad 7) Czy planowane są działania legislacyjne dotyczące przeciwdziałania wykorzystaniu technologii deepfake w działalności przestępczej?

Penalizacja przestępstw z wykorzystaniem deepfake leży w kompetencjach Ministra Sprawiedliwości, z którym Ministerstwo Cyfryzacji współpracuje.

Ministerstwo Sprawiedliwości w dniu 22 grudnia 2025 r. zwróciło się do Komisji Kodyfikacyjnej Prawa Karnego (dalej jako: „KKPK") z prośbą o wydanie opinii, czy obecne przepisy prawnokarne w wystarczający sposób penalizują kwestie rozpowszechniania

deepfake'ów przy użyciu sztucznej inteligencji (np. poprzez ustawę Kodeks karny[1]) i czy niezbędne jest spenalizowanie nowego typu przestępstwa, a jeśli tak - zaproponowanie jego brzmienia. Ponadto Ministerstwo Sprawiedliwości zostało poinformowane o potrzebie zmian legislacyjnych dotyczących ochrony przed treściami generowanymi przez AI, w tym treściami typu CSAM.

Ministerstwo Cyfryzacji uczestniczy w pracach nad unijnymi ramami przejrzystości AI, które tworzą mechanizmy prewencyjne, a już w szczególności obowiązek znakowania treści syntetycznych wynikający z art. 50 AI Act, który oczekuje na wejście w życie.

Niezależnie od prac KKPK, zasadnicze znaczenie dla oceny potrzeby krajowych działań legislacyjnych mają trwające prace nad zmianą art. 5 AI Act w ramach pakietu Digital Omnibus on AI. Komisja Europejska zaproponowała rozszerzenie katalogu praktyk w zakresie AI bezwzględnie zakazanych na terytorium UE o:

I. zakaz systemów AI generujących niekonsensualnych intymnych treści wizualnych (NCII);

II. zakaz systemów AI generujących materiały przedstawiające seksualne wykorzystywanie dzieci (CSAM), w tym treści syntetyczne.

Polska popiera proponowane rozszerzenia i uczestniczy aktywnie w pracach na forum Rady UE. Rozporządzenie UE stosowane jest bezpośrednio — po wejściu w życie zmienionego art. 5 AI Act przepisy te będą obowiązywać wprost w polskim porządku prawnym, bez potrzeby odrębnej legislacji krajowej w zakresie właściwości zakazanych systemów AI.

Polityka AI zakłada budowę otwartych ram dla innowacji z poszanowaniem godności człowieka, uczciwej konkurencji i odporności społecznej, zgodnie z AI Act oraz Ramową konwencją Rady Europy w sprawie sztucznej inteligencji, praw człowieka, demokracji i praworządności.

Ad 8) Czy prowadzone są programy edukacyjne mające na celu zwiększenie świadomości obywateli w zakresie rozpoznawania manipulacji cyfrowych?

Ministerstwo Cyfryzacji prowadzi kampanię społeczną *Przepis na dezinformację*, której celem jest rozwijanie umiejętności krytycznej oceny treści w sieci, w tym treści syntetycznych i zmanipulowanych.

Edukacja cyfrowa jest integralnym elementem Polityki AI. Cel 5 przewiduje stworzenie ogólnodostępnego narzędzia do przeciwdziałania dezinformacji AI (wskaźnik monitorowany do 2030 r.). Budowanie świadomości obywateli w zakresie odpowiedzialnej AI należy do kluczowych zadań ministra właściwego ds. informatyzacji jako organu koordynującego Politykę AI.

Budowanie kompetencji w zakresie rozumienia systemów AI (*AI literacy*) jest jednocześnie jednym z priorytetów unijnej polityki cyfrowej, z którą Polityka AI jest spójna.

Ad 9) Czy Ministerstwo analizuje potencjalny wpływ technologii deepfake na procesy demokratyczne oraz bezpieczeństwo informacyjne państwa?

Ministerstwo Cyfryzacji analizuje wpływ treści generowanych przez AI (w tym deepfake) na procesy demokratyczne i bezpieczeństwo informacyjne w wymiarze prawno-regulacyjnym i strategicznym: chodzi o ochronę praw podstawowych, integralność przestrzeni informacyjnej i odporność społeczną na dezinformację.

[1] Art. 190a § 2-3, art. 202 § 4b ustawy z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2025 r. poz. 383) (dalej jako: „k.k.")

Polityka AI identyfikuje szybkie rozprzestrzenianie się dezinformacji jako wyzwanie dla bezpieczeństwa AI i wskazuje działania edukacyjne jako warunek zaufania obywatelskiego. Cel 5 obejmuje monitoring wpływu AI na społeczeństwo we współpracy z NASK, GUS, PIE i IBE. Planowane jest także uczestnictwo w europejskim AI Observatory, które będzie gromadzić dane o skutkach wdrażania AI, w tym dla sfery informacyjnej. Bezpieczeństwo informacyjne w wymiarze operacyjnym pozostaje w kompetencjach służb odpowiedzialnych za bezpieczeństwo wewnętrzne i cyberbezpieczeństwo.

Ad 10) Jak Ministerstwo ocenia poziom przygotowania instytucji publicznych do przeciwdziałania zagrożeniom wynikającym z rozwoju technologii deepfake?

Wdrożenie AI Act – a wraz z nim obowiązek znakowania treści syntetycznych (art. 50) i planowany Kodeks Przejrzystości – stworzy skoordynowane standardy dla całego ekosystemu: zarówno dla dostawców technologii, jak i organów nadzoru.

Na poziomie krajowym kompetencje w zakresie bezpieczeństwa AI buduje NASK w ramach Ośrodka Badań nad Bezpieczeństwem AI oraz inne jednostki B+R, zgodnie z Polityką AI (sekcja 4.4). Polityka AI zakłada ponadto wdrożenie norm ISO/IEC 27090 (bezpieczeństwo systemów AI) i ISO/IEC 42001 (systemy zarządzania AI) w administracji publicznej i u operatorów infrastruktury krytycznej.

Z wyrazami szacunku
Dariusz Standerski
Sekretarz Stanu
/dokument podpisany elektronicznie/

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