Ministerstwo
Cyfryzacji

Sekretarz Stanu
Dariusz Standerski

BM.WP.057.24.2026
Warszawa, 08 marca 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 29 stycznia br. Posłanki na Sejm RP Pani Moniki Rosy w sprawie przeciwdziałania rozpowszechnianiu treści typu deepfake w Internecie i ochrony danych osobowych (interpelacja nr 14897)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłankę pytania.

Ad 1) Czy Ministerstwo Cyfryzacji prowadzi obecnie prace nad przygotowaniem odrębnych regulacji prawnych dedykowanych przeciwdziałaniu tworzeniu i rozpowszechnianiu treści typu deepfake, w szczególności z wykorzystaniem wizerunku i głosu osób fizycznych?

Ministerstwo Cyfryzacji prowadziło prace nad nowelizacją ustawy o świadczeniu usług drogą elektroniczną, mającą na celu umożliwienie stosowania przepisów rozporządzenia Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), dalej jako „DSA". Dnia 9 stycznia br. ustawa została zawetowana przez Prezydenta RP.

Ministerstwo Cyfryzacji przygotowało nowe projekty wdrażające DSA. Przepisy zostały ujęte w dwóch projektach, aby przyspieszyć wdrożenie. Projekty ustaw zostały już wpisane do wykazu prac legislacyjnych i programowych Rady Ministrów pod numerami UC140 i UC141 i od 6 lutego 2026 r. rozpoczęły się oficjalne uzgodnienia i konsultacje obu projektów. Projekty zostały opublikowane na stronie Rządowego Centrum Legislacji.[1]

Jednym z elementów nowelizacji jest wprowadzenie procedury wydawania nakazów podjęcia działań przeciwko nielegalnym treściom polegających na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Wniosek o wydanie takiego nakazu będzie mógł złożyć do Prezesa Urzędu Komunikacji Elektronicznej lub Przewodniczącego Krajowej Rady Radiofonii i Telewizji (w zakresie treści występujących w usłudze świadczonej przez platformę udostępniania wideo w rozumieniu art. 4 pkt 22a ustawy z dnia 29 grudnia 1992 r. o radiofonii i telewizji) prokurator, Policja, organ Krajowej Administracji Skarbowej, usługobiorca lub uprawniony z tytułu praw autorskich i praw pokrewnych. Co istotne, wniosek będzie mógł dotyczyć wyłącznie treści, których rozpowszechnianie może wyczerpywać znamiona określonych czynów zabronionych (a także nawołujących do popełnienia takie czynu zabronionego lub pochwalających jego popełnienie). Wśród wymienionych w art. 11a ust. 1 pkt 1 nowelizowanej ustawy czynów zabronionych znalazły się między innymi czyny, których znamiona może wypełniać stosowanie technologii deepfake, a mianowicie:

— art. 190a § 2 Kodeksu karnego, który obejmuje wykorzystanie wizerunku pokrzywdzonego, tak jakby uczynił to on sam w swoim imieniu, przez co wyrządza jej szkodę majątkową lub osobistą;

[1] https://legislacja.rcl.gov.pl/projekt/12406906 oraz https://legislacja.rcl.gov.pl/projekt/12406905

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

ul. Królewska 27
00-060 Warszawa

- art. 191a § 1 Kodeksu karnego, który obejmuje utrwalanie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej, używając w tym celu wobec niej przemocy;
- groźby bezprawnej lub podstępu, albo rozpowszechnianie wizerunku nagiej osoby lub osoby w trakcie czynności seksualnej bez jej zgody;
- art. 202 § 1, 3–4c Kodeksu karnego, który dotyczy publicznego prezentowania, produkcji, rozpowszechniania, przechowywania treści pornograficznych, zwłaszcza z udziałem małoletnich. W kontekście możliwości popełnienia tego przestępstwa obejmuje on dystrybucję pornografii dziecięcej przez internet, przechowywanie takich treści na serwerach;
- art. 286 § 1 i 2 Kodeksu karnego, który dotyczy doprowadzenia do niekorzystnego rozporządzenia mieniem przez wprowadzenie w błąd. Obejmuje on phishing, oszustwa na platformach sprzedażowych.

Wprowadzenie powyższej procedury da realne narzędzia do walki z negatywnymi przypadkami wykorzystania technologii deepfake przy jednoczesnym zachowaniu szybkości i transparentności postępowania.

Warto dodać, że instrumentem prawnym regulującym kwestie generowania i rozpowszechniania treści typu deepfake na poziomie unijnym jest akt o sztucznej inteligencji (AI Act), który określa:

a) Systemy zakazane (art. 5 AI Act), czyli wskazane wprost w rozporządzeniu zakazy dotyczące stosowania systemów AI wykorzystujących techniki podprogowe lub manipulacyjne;
b) Obowiązki w zakresie przejrzystości wynikające z motywu 134 i art. 50 AI Act przewidują obowiązek oznaczania treści wygenerowanych przez AI (w tym deepfake'ów), tak aby użytkownik miał świadomość kontaktu z treścią nieprawdziwą. Należy jednak zaznaczyć, że zgodnie z art. 113 AI Act obowiązki te powinny w pełni wejść w życie 2 sierpnia br. Na tę datę mogą mieć jednak wpływ postanowienia wynikające z procedowanego obecnie projektu *Digital Omnibus on AI*, czyli zaprezentowanego w listopadzie 2025 r. pakietu uproszczeń do AI Act.

Należy także podkreślić, że zagadnienia dotyczące funkcjonowania systemów sztucznej inteligencji, w tym mechanizmów zapobiegania nadużyciom technologicznym, odpowiedzialności systemowej platform cyfrowych czy szczegółowych rozwiązań technicznych służących wykrywaniu treści generowanych lub modyfikowanych przy użyciu AI w zakresie, w jakim treści te zawierają informacje pozwalające na identyfikację osoby fizycznej – w tym jej wizerunek lub głos – podlegają reżimowi ochrony danych osobowych.

Wszelkie informacje, w zakresie w jakim zawierają informacje pozwalające na identyfikację osoby fizycznej, stanowią dane osobowe w rozumieniu art. 4 pkt 1 rozporządzenia (UE) 2016/679 (RODO) i podlegają zasadom przetwarzania danych określonym w tym rozporządzeniu. Dotyczy to również treści generowanych, modyfikowanych lub rozpowszechnianych przy wykorzystaniu narzędzi opartych na sztucznej inteligencji, jeżeli umożliwiają one identyfikację osoby fizycznej, w szczególności poprzez wizerunek lub głos.

Przetwarzanie takich danych osobowych musi odbywać się zgodnie z zasadami określonymi w art. 5 RODO, w szczególności zasadą legalności, rzetelności i przejrzystości, minimalizacji danych oraz ograniczenia celu. Każde przetwarzanie wymaga również istnienia odpowiedniej podstawy prawnej, o której mowa w art. 6 RODO, a w przypadku danych szczególnych kategorii – spełnienia dodatkowych przesłanek określonych w art. 9 ust. 1 i 2 RODO.

Podmiot, który decyduje o celach i sposobach przetwarzania danych osobowych – w tym o wykorzystaniu narzędzi AI do tworzenia, modyfikowania lub publikowania treści zawierających dane osobowe – może zostać uznany za administratora danych w rozumieniu art. 4 pkt 7 RODO, ewentualnie za współadministratora lub podmiot przetwarzający, w zależności od konkretnego modelu przetwarzania. W konsekwencji ponosi on odpowiedzialność za zgodność przetwarzania z przepisami RODO, w tym za realizację obowiązków wynikających z art. 32 RODO, dotyczących stosowania odpowiednich środków technicznych i organizacyjnych zapewniających bezpieczeństwo danych osobowych.

W kontekście dzieci i młodzieży należy podkreślić, że RODO przewiduje szczególny poziom ochrony danych osobowych małoletnich, co powinno być uwzględniane zarówno przy ocenie legalności przetwarzania, jak i przy doborze środków zabezpieczających oraz ocenie ryzyka dla praw i wolności osób, których dane dotyczą.

W konsekwencji należy wskazać, że RODO w sposób kompleksowy i spójny określa zasady przetwarzania danych osobowych oraz odpowiedzialność podmiotów uczestniczących w tym przetwarzaniu, niezależnie od technologii wykorzystywanej w procesie przetwarzania danych. W tym zakresie obowiązujące przepisy prawa ochrony danych osobowych zapewniają czytelne i wystarczające ramy prawne, umożliwiające ocenę legalności przetwarzania danych osobowych oraz egzekwowanie odpowiednich obowiązków. Wobec tego Ministerstwo Cyfryzacji nie identyfikuje obecnie potrzeby podejmowania odrębnych krajowych prac legislacyjnych w obszarze ochrony danych osobowych w tym wymiarze.

Ad 2) W jaki sposób Ministerstwo Cyfryzacji zamierza zapewnić skuteczną i szybką ochronę ofiar deepfake'ów, w tym dzieci i młodzieży, przed długotrwałym rozpowszechnianiem nieprawdziwych i krzywdzących materiałów w internecie?

Ministerstwo Cyfryzacji bierze aktywny udział w pracach na forum unijnym w zakresie powstających regulacji, jak i egzekwowania obowiązujących przepisów. Zidentyfikowane zagrożenia związane z wykorzystaniem deepfake'ów objęte są regulacjami m.in. Rozporządzenia (UE) 2022/2065 w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), jak i Rozporządzenia (UE) 2024/1689 z dnia 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). Oba rozporządzenia obowiązują bezpośrednio w całej Unii Europejskiej, chociaż wymagają formalnego dostosowania krajowych porządków prawnych do wprowadzanych rozwiązań. W związku z tym Ministerstwo Cyfryzacji przygotowało projekt ustawy, której celem jest ustanowienie procedury wydawania nakazów uniemożliwienia dostępu do treści nielegalnych w rozumieniu Aktu o usługach cyfrowych. Procedura dotyczy m.in. treści, których rozpowszechnianie może wyczerpywać znamiona czynów zabronionych określonych w ustawie – Kodeks karny, takich jak: art. 190a § 2 (kradzież tożsamości); art. 191a § 1 (naruszenie intymności seksualnej); art. 200 § 3 i 5 (prezentowanie treści pornograficznych małoletnim); art. 202 § 1 (publiczne prezentowanie treści pornograficznych); art. 286 § 1 i 2 (oszustwo). Wskazane czyny zabronione mogą wiązać się także z wykorzystaniem deepfake'ów w ramach tych treści. Ustawa umożliwiłaby więc usunięcie lub uniemożliwienie dostępu do takich nielegalnych treści, przy jednoczesnym zachowaniu prawa do sprzeciwu. W odniesieniu do możliwych sankcji trzeba wskazać, że możliwe będzie zablokowanie dostępu do usługi dostawcy niewywiązującego się z nakazu uniemożliwienia dostępu do nielegalnych treści.

Obok tego Akt w sprawie sztucznej inteligencji wymaga aby treści, które mogą niesłusznie zostać uznane przez odbiorcę za autentyczne lub prawdziwe, zostały odpowiednio oznakowane jako wygenerowane lub zmanipulowane przez AI lub zostało w inny sposób ujawnione, że ich źródłem jest AI. Jest to obowiązek przewidziany w art. 50 aktu, nałożony na podmioty stosujące system AI umożliwiający generowanie obrazów, treści audio lub wideo stanowiące treści deepfake.

Jednocześnie należy podnieść, że zarówno dla unijnej, jak i krajowej legislacji, wyzwanie stanowi odpowiednie przystosowanie prawa do zmian technologicznych. Dodatkowo jednym z głównych problemów jest brak odpowiednich narzędzi umożliwiających skuteczne identyfikowanie zmanipulowanych treści w czasie rzeczywistym. Wciąż rozwijane technologie pozwalające na stworzenie deepfake wymagać będą coraz silniejszych zabezpieczeń umożliwiających wykrycie i usunięcie tych treści, nieodzowne może więc okazać się zintensyfikowanie nakładów i działań ze strony odpowiednich służb krajowych w tym zakresie.

Co istotne, NASK-PIB prowadzi serwis internetowy dyzurnet.pl stanowiący punkt kontaktowy do przyjmowania zgłoszeń dotyczących nielegalnych treści w internecie. Dyzurnet.pl umożliwia zgłaszanie materiałów przestawiających seksualne wykorzystywanie dzieci, twardej pornografii, rasizmu i ksenofobii, innych nielegalnych treści. Ponadto poza ww. nielegalnymi treściami serwis umożliwia zgłaszanie treści szkodliwych, do których zaliczają się m.in.:

1) treści prezentujące przemoc, zachowania agresywne, obrażenia fizyczne, deformacje ciała, np. zdjęcia z wypadków, okrucieństwo wobec zwierząt,
2) treści zawierające elementy psychomanipulacji, czyli sterowania cudzymi uczuciami, którego celem jest wyłudzenie korzyści materialnych lub zmuszenie do niewłaściwych, często ryzykownych zachowań.

Działalność punktu kontaktowego umożliwia blokowanie dostępu do nielegalnych treści jak i przekazywanie informacji Policji. Ponadto w ramach funkcjonowania punktu prowadzony jest szereg inicjatyw edukacyjnych mających na celu popularyzację wiedzy na temat bezpiecznego korzystania z internetu.

Niezależnie od powyższego, Ministerstwo Cyfryzacji prowadzi szereg działań i projektów edukacyjnych mających na celu walkę z dezinformacją, w tym także dezinformacją opartą o wykorzystanie narzędzi AI i deepfake'ów. Ponadto, walka z dezinformacją stanowi jeden z filarów Strategii Cyfryzacji Państwa, zdefiniowany w ramach bezpiecznej przestrzeni cyfrowej.

W przypadku pojawienia się spreparowanych materiałów z udziałem dzieci, ich rodzice i opiekunowie mogą:

- zgłaszać treści do zespołu Dyżurnet działającego w ramach NASK (https://dyzurnet.pl/zglos-nielegalne-tresci/?pl) oraz korzystać z mechanizmów zgłaszania na platformach internetowych;
- składać zawiadomienia do Policji lub prokuratury – w przypadku podejrzenia popełnienia przestępstwa;
- korzystać z poradników przygotowywanych przez zespół NASK dotyczących kwestii bezpieczeństwa np. w zakresie ochrony wizerunku dziecka w sieci (https://www.gov.pl/web/niezagubdzieckawsieci/sharenting-i-wizerunek-dziecka-w-sieci).

Ad 3) Czy planowane jest nałożenie na operatorów platform internetowych i mediów społecznościowych dodatkowych obowiązków w zakresie proaktywnej identyfikacji,

oznaczania oraz usuwania treści deepfake, w szczególności takich, które naruszają prawa małoletnich?

Ad 4) Czy Ministerstwo Cyfryzacji analizuje możliwość wprowadzenia sankcji administracyjnych lub cywilnych wobec podmiotów, które nie zapewniają skutecznych mechanizmów przeciwdziałania rozpowszechnianiu deepfake'ów na zarządzanych przez siebie platformach?

Jak zostało wskazane w odpowiedzi na pytanie nr 2 Ministerstwo Cyfryzacji bierze aktywny udział w pracach na forum unijnym w zakresie powstających regulacji, jak i egzekwowania obowiązujących przepisów.

Warto podkreślić, że w ramach AI Act operatorzy będą zobowiązani do wdrażania mechanizmów identyfikacji i oznaczania deepfake'ów, co ułatwi ich późniejszą moderację (co zostało już omówione w odpowiedzi na pytanie nr 1). Obecnie trwają prace nad projektem ustawy o systemach sztucznej inteligencji, który wyznaczy krajowy organ nadzoru rynku nad systemami sztucznej inteligencji odpowiedzialny m.in. za prowadzenie postępowań, kontrole oraz nakładanie administracyjnych kar pieniężnych.

Jednocześnie, odnosząc się do pytań nr 3 i 4, należy wspomnieć o postępowaniu, które Komisja Europejska wszczęła w styczniu br. na podstawie DSA wobec platformy X. Postępowanie ma na celu ocenę, czy firma właściwie oceniła i zminimalizowała ryzyko związane z wdrożeniem funkcjonalności Grok w systemie X w UE. Obejmuje to ryzyko związane z rozpowszechnianiem nielegalnych treści, takich jak zmanipulowane obrazy o charakterze seksualnym, w tym treści, które mogą być materiałami przedstawiającymi wykorzystywanie seksualne dzieci.

Komisja Europejska będzie dalej badać, czy X wywiązuje się ze swoich obowiązków wynikających z DSA w zakresie:

- starannej oceny i ograniczania ryzyka systemowego, w tym związanego z rozpowszechnianiem nielegalnych treści, negatywnymi skutkami przemocy ze względu na płeć oraz poważnymi negatywnymi konsekwencjami dla dobrostanu fizycznego i psychicznego wynikającymi z wdrożenia funkcji Grok na platformie;
- przeprowadzenia i przekazania Komisji Europejskiej sprawozdania ad hoc z oceny ryzyka w odniesieniu do funkcji Grok w usłudze X, które mają krytyczny wpływ na profil ryzyka X przed ich wdrożeniem.

Ponadto, Komisja rozszerzyła toczące się formalne postępowanie wszczęte przeciwko X w grudniu 2023 r., aby ustalić, czy X właściwie ocenił i złagodził wszystkie ryzyka systemowe, określone w akcie o usługach cyfrowych, związane z jego systemami rekomendacji, w tym wpływ niedawno ogłoszonego przejścia na system rekomendacji oparty na systemie Grok.

W przypadku udowodnienia tych uchybień stanowiłyby one naruszenie art. 34 ust. 1 i 2, art. 35 ust. 1 i art. 42 ust. 2 DSA.

Ad 5) Czy przewidywane są działania o charakterze edukacyjnym i systemowym, realizowane we współpracy z innymi resortami, organami ochrony danych oraz instytucjami odpowiedzialnymi za ochronę dzieci i młodzieży, mające na celu zwiększenie świadomości społecznej na temat zagrożeń związanych z technologią deepfake?

Zgodnie z wynikami badań przeprowadzonych przez NASK, wraz z dorastaniem małoletnich wzrasta ich świadomość i umiejętność oceny wiarygodności informacji w internecie – co jednak wymaga ciągłego wsparcia w postaci systematycznych działań edukacyjnych nakierowanych na pogłębienie kompetencji informacyjnych wśród najmłodszych. Obecnie działania takie podejmowane są m.in. przez NASK, prowadzący w

szkołach szkolenia dla dzieci – w tym dotyczące m.in. dezinformacji – w ramach Cyberprofilaktyki NASK. Uzupełniająco oferowane są w ramach OSE IT Szkoła materiały szkoleniowe dla młodzieży i nauczycieli (Ogólnopolska Sieć Edukacyjna to publiczna sieć telekomunikacyjna obejmującą szkoły podstawowe i ponadpodstawowe, gwarantująca szkołom dostęp do szybkiego, bezpłatnego i bezpiecznego internetu; OSE zawiera również wiele treści edukacyjnych, w tym scenariusze lekcji dla nauczycieli o cyberzagrożeniach).

Na platformie e-learningowej OSE dostępny jest kurs dla uczniów szkół ponadpodstawowych i nauczycieli „Dezinformacja", który powstał w ramach ogólnopolskiego projektu „Broń się w necie", realizowanego przez Państwowy Instytut Badawczy NASK oraz Ministerstwo Cyfryzacji we współpracy z Agencją Bezpieczeństwa Wewnętrznego: https://it-szkola.edu.pl/news,art,904. Kurs obejmuje między innymi naukę korzystanie z narzędzi do samodzielnej weryfikacji informacji oraz innych materiałów w internecie, w tym generowanych przez sztuczną inteligencję.

Dezinformacja związana z wykorzystaniem deepfake'ów stanowi zagrożenie dla całego społeczeństwa, a zwłaszcza dzieci. Nieodzowne jest kontynuowanie warsztatów i kursów przeznaczonych dla dzieci, ich opiekunów, nauczycieli, jak i urzędników i funkcjonariuszy. Niezależnie od tego organizowane są kampanie społeczne – tak jak kampania NASK dot. fake newsów, które bardzo często wykorzystują materiały typu deepfake. Obok tego przez Ministra Cyfryzacji finansowane są inne szkolenia wykonywane przez NASK, mające na celu rozwój kompetencji cyfrowych funkcjonariuszy i pracowników Policji i Państwowej Straży Pożarnej – takie szkolenia realizowane są w obszarze sztucznej inteligencji, dezinformacji, cyberbezpieczeństwa oraz cyberhigieny.

Ponadto, Ministerstwo Cyfryzacji prowadzi stałą, bieżącą współpracę z Prezesem Urzędu Ochrony Danych Osobowych w sprawach dotyczących ochrony danych osobowych oraz stosowania przepisów RODO. Obecnie priorytetem jest analiza oraz opracowanie uproszczeń w ramach tzw. omnibusa cyfrowego, obejmującego również propozycje zmian w RODO, a także analiza rozporządzenia Parlamentu Europejskiego i Rady (UE) 2025/2518 z dnia 26 listopada 2025 r. w sprawie ustanowienia dodatkowych przepisów proceduralnych dotyczących egzekwowania RODO, pod kątem ewentualnej konieczności nowelizacji prawa krajowego.

Ad 6) Jak Ministerstwo Cyfryzacji ocenia adekwatność obecnych przepisów prawa krajowego w zestawieniu z rosnącą skalą nadużyć wykorzystujących sztuczną inteligencję oraz jakie kierunki zmian legislacyjnych uznaje za priorytetowe w najbliższym czasie?

Tak jak wskazano w poprzednich punktach, Ministerstwo Cyfryzacji dostrzega problem nadużyć związanych z wykorzystywaniem sztucznej inteligencji, zwłaszcza w zakresie dezinformacji i powstawania deepfake. Z tego powodu zapewniane są odpowiednie szkolenia i materiały edukacyjne w tym zakresie, zwłaszcza kierowane do dzieci i nauczycieli. Jednocześnie nieodzowne jest przystosowanie polskiego porządku prawnego do obowiązujących unijnych rozporządzeń, w tym Aktu o usługach cyfrowych i Aktu w sprawie sztucznej inteligencji. Jak zwrócono także uwagę w odpowiedzi na pytanie pierwsze, z punktu widzenia Ministerstwa Cyfryzacji nieodzowne jest wprowadzenie w pierwszej kolejności rozwiązań z zakresu ograniczenia dostępu do treści pornograficznych w internecie (jako treści lepiej zbadanych i łatwiejszych w zidentyfikowaniu), przed podjęciem prac nad uregulowaniem treści szkodliwych oraz deepfake'ów – w przypadku których wykorzystać będzie można rozwiązania sprawdzone po uchwaleniu ustawy o ochronie małoletnich przed dostępem do treści pornograficznych w internecie.

Ministerstwo Cyfryzacji zidentyfikowało luki regulacyjne w zakresie wskazywanych na płaszczyźnie interpelacji problemów w związku z czym opracowane zostały propozycje

legislacyjnej wskazane w odpowiedzi na pytanie nr 1. Jednocześnie w ramach MC prowadzone są prace nad wprowadzeniem do systemu prawnego regulacji zapewniającej koherentne uregulowanie zastosowania systemów AI w RP, tj. ustawy o systemach sztucznej inteligencji.

Prace nad projektem ustawy o systemach sztucznej inteligencji są na zaawansowanym etapie. Głównym celem jest zapewnienie bezpiecznego rozwoju AI przy jednoczesnym zabezpieczeniu praw podstawowych obywateli, co w połączeniu z działaniami MC w zakresie nowej wersji ustawy wdrażającej DSA ma stanowić kompleksową odpowiedź na nadużycia technologiczne.

Ad 7) Czy Ministerstwo Cyfryzacji planuje podjęcie działań legislacyjnych lub interpretacyjnych zmierzających do implementacji do polskiego porządku prawnego rekomendacji oraz standardów ochrony wynikających z wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 2 grudnia 2025 r. w sprawie C-492/23 (Russmedia), w szczególności w zakresie odpowiedzialności platform internetowych za treści zawierające dane osobowe oraz skutecznych mechanizmów ich szybkiego usuwania?

W dniu 30 grudnia 2025 r. Ministerstwo Cyfryzacji przedstawiło stanowisko w sprawie przedmiotowego wyroku wskazując, że nie dostrzega potrzeby zmiany obowiązującego w Polsce prawa w zakresie właściwości Ministra Cyfryzacji. Uzasadniając to tym, że ww. wyrok nie implikuje konieczności zmian przepisów krajowych z uwagi na fakt, że RODO stosuje się bezpośrednio, a przedstawiona przez TSUE interpretacja jedynie doprecyzowuje istniejące obowiązki. Przedmiotowy wyrok może natomiast wskazywać na potrzebę dostosowania praktyki stosowania prawa przez operatorów platform oraz uwzględnienia tej wykładni w działaniach organu nadzorczego przy ocenie stosowanych środków technicznych i organizacyjnych.

W odniesieniu do wyroku Trybunału Sprawiedliwości Unii Europejskiej z dnia 2 grudnia 2025 r. w sprawie C-492/23 (Russmedia) należy wskazać, że orzeczenie to potwierdza fundamentalne założenia prawa ochrony danych osobowych, zgodnie z którymi podmioty decydujące o celach i sposobach przetwarzania danych osobowych ponoszą odpowiedzialność za zgodność tego przetwarzania z RODO, w tym za zapewnienie odpowiednich środków ochrony danych osobowych.

Wyrok ten wpisuje się w utrwaloną linię orzeczniczą, zgodnie z którą administrator danych nie może uchylać się od odpowiedzialności za przetwarzanie danych osobowych wyłącznie z uwagi na charakter technologii wykorzystywanej do publikowania lub rozpowszechniania treści, w tym technologii opartych na sztucznej inteligencji.

Orzeczenie to nie ustanawia nowych norm prawnych ani nie nakłada na państwa członkowskie obowiązku zmiany obowiązujących przepisów, lecz wpisuje się w utrwaloną linię orzeczniczą dotyczącą odpowiedzialności podmiotów uczestniczących w przetwarzaniu danych osobowych.

Przywołany wyrok nie dotyczy sposobu wdrożenia przepisów dyrektywy 2000/31/WE w sprawie niektórych aspektów prawnych usług społeczeństwa informacyjnego, w szczególności handlu elektronicznego w ramach rynku wewnętrznego (dyrektywa o handlu elektronicznym) w poszczególnych państwach członkowskich, lecz interpretacji brzmienia tych przepisów w ich rozumieniu wskazanym w tej dyrektywie. Polskie przepisy wdrażające dyrektywę o handlu elektronicznym wprowadzają bowiem takie same uprawnienia co te przewidziane w art. 12-15 tej dyrektywy. Ponadto obecnie obowiązującymi, analogicznymi przepisami do tych stanowiących podstawę wykładni Trybunału Sprawiedliwości Unii Europejskiej są przepisy Aktu o usługach cyfrowych, bezpośrednio obowiązujących w całej Unii Europejskiej.

Jednakże przeprowadzona przez Trybunał Sprawiedliwości Unii Europejskiej wykładnia potencjalnie wpłynie na praktykę stosowania prawa w Unii Europejskiej, w tym także w Polsce. Zobowiązanie operatorów internetowych platform handlowych – w zakresie w jakim są administratorami danych – do weryfikowania czy w ogłoszeniach zawieranych na ich platformach znajdują się dane osobowe szczególnej kategorii oraz weryfikowania tożsamości użytkowników publikujących ogłoszenia zawierające dane osobowe potencjalnie rozszerzy zasady ochrony danych osobowych, uszczegóławiając zobowiązania po stronie administratorów. Należy jednak wskazać, że dotyczy to szczegółowo określonych sytuacji. Jak podkreślił bowiem Trybunał Sprawiedliwości Unii Europejskiej, bycie podmiotem obowiązków przewidzianych w ogólnym rozporządzeniu o ochronie danych, nie wyklucza automatycznie możliwości powołania się na art. 12–15 dyrektywy o handlu elektronicznym w odniesieniu do kwestii innych niż dotyczące ochrony danych osobowych.

Prawidłowość powołania się na to wyłączenie wymagać będzie jednak każdorazowej oceny ze strony organu nadzoru – Prezesa Urzędu Ochrony Danych Osobowych – w przypadku kontroli przestrzegania przepisów ochrony danych osobowych przez dostawców prowadzących internetowe platformy handlowe z ogłoszeniami. W tym zakresie zarówno tacy dostawcy, jak i Prezes Urzędu Ochrony Danych Osobowych, będą musieli odpowiednio wyważyć zakres obowiązków nakładanych w ogólnym rozporządzeniu o ochronie danych z charakterem oferowanych usług, dokonując analizy czy w danej sytuacji przepisy tego rozporządzenia wykluczają możliwość powołania się na wyłączenie z odpowiedzialności za treści przechowywane w usługach, określone w dyrektywie o handlu elektronicznym i akcie o usługach cyfrowych. W tym zakresie konieczne będzie m.in. wzięcie pod uwagę uprawnień dostawców względem zamieszczanych w usłudze treści, określanych w ogólnych warunkach świadczenia usługi istotnych sposobów opublikowania odnośnych danych osobowych oraz rzeczywistego zakresu działania ze strony dostawców względem treści zamieszczanych w usłudze, w szczególności wykorzystywania tych treści w celach reklamowych i handlowych. Dodatkowo w przypadku stwierdzenia, że dostawca internetowych platform handlowych powinien stosować środki zabezpieczające ochronę danych osobowych, Prezes Urzędu Ochrony Danych Osobowych będzie musiał wziąć pod uwagę charakter tych środków, w tym czy zostały wdrożone z uwzględnieniem różnych kryteriów wskazanych w przepisach ochrony danych osobowych oraz potrzeb ochrony danych konkretnie związanych z danym przetwarzaniem, a także ryzyka wynikającego z tego przetwarzania.

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