



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.13.2026
Warszawa, 09 kwietnia 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 20 stycznia 2026 r. Pośła na Sejm RP Pana Tadeusz Samborski w sprawie reagowania na przypadki szerzenia dezinformacji za pośrednictwem kont internetowych podszywających się pod oficjalne profile internetowe jednostki samorządu terytorialnego (interpelacja nr 14650)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Na wstępie pragnę zaznaczyć, że Minister Cyfryzacji nie posiada uprawnień śledczych czy też możliwości prowadzenia działań operacyjnych takich jak odpowiednie ku temu służby.

Ad 1) Czy jest zgodny z przepisami i obowiązującymi regułami taki stan rzeczy gdy obok oficjalnego profilu „Gminy Prochowice”, równoległe na tym samym portalu społecznościowym (Facebook) funkcjonuje profil pod nazwą „Prochowice”?
Podobieństwo nazw, używanie herbu gminnego czy sposobu komunikacji stwarza realne ryzyko wprowadzenia w błąd odbiorców co do charakteru i wiarygodności publikowanych treści, sprzyjając dalszemu rozpowszechnianiu dezinformacji. Oficjalne profile jednostek samorządu terytorialnego w swoim działaniu mają na celu informowanie czytelników o swojej bieżącej działalności. Równoległe działanie dwóch kont o zbliżonej nazwie, tematyce, a także sposobie komunikacji, może doprowadzić do mylnego przypisywania dezinformacyjnych treści oficjalnemu kontu. Taka narracja tworzy przestrzeń do uznania, iż cała działalność jednostki samorządu terytorialnego nie jest spójna i dawać złudzenie, że dezinformacyjne, nienawistne wpisy są publikowane przez oficjalny profil społecznościowy miasta Prochowice.

W obowiązującym porządku prawnym brak jest przepisu zakazującego wprost funkcjonowania w mediach społecznościowych profili niebędących oficjalnymi kanałami jednostki samorządu terytorialnego, nawet jeśli nazwa profilu jest zbliżona do nazwy gminy. Nie oznacza to jednak, że możliwe jest dowolne wykorzystywanie symboliki samorządowej lub wprowadzanie użytkowników w błąd. W tym zakresie zastosowanie znajdują następujące regulacje prawa które pozwalają Administracji publicznej na stosowne działania. Z Pana pisma wynika, iż oprócz podobieństwa nazwy (brak wyróżnika JST) wskazany profil wykorzystuje herb Gminy, co może stanowić naruszenie Ochrony herbu gminy i symboli JST. Jednostki samorządu terytorialnego mogą na podstawie art. 3 ust. 1 ustawy z dnia 21 grudnia 1978 r. o odznakach i mundurach (Dz. U. Nr 31, poz. 130, z późn. zm.) w drodze uchwały ustanowić własny herb, flagę, emblematy oraz insygnia i inne symbole. Natomiast ustawa o samorządzie gminnym w art. 18 ust. 2 pkt 13 stanowi, że do wyłącznej właściwości rady gminy należy: m.in. podejmowanie uchwał w sprawach herbu gminy, a co za tym idzie jeżeli nie jest to dozwolone gmina może dochodzić swoich praw w zakresie używania herbu na drodze cywilnej,

- dóbr osobistych osoby prawnej (tj. gminy) w rozumieniu art. 23 i 24 Kodeksu cywilnego,
- autorskich praw majątkowych lub znaków towarowych, jeśli herb został zarejestrowany np. w Urzędzie Patentowym.

W odniesieniu do wprowadzanie odbiorców w błąd w przypadku treści i działań wywołujących efekt mylnego utożsamiania profilu z oficjalnym kanałem gminy, znajduje zastosowanie:

- art. 24 § 1 Kodeksu cywilnego – ochrona dóbr osobistych, w tym dobrego imienia jednostki samorządowej,
- art. 190a § 2 Kodeksu karnego, jeżeli dochodzi do podszywania się („podszywa się pod inną osobę w celu wyrządzenia szkody majątkowej lub osobistej”).

Należy jednak podkreślić, że powyższe działania leżą w kompetencji JST a nie Ministra Cyfryzacji.

W odniesieniu do wpisów noszących znamiona dezinformacji w polskiej infosferze dezinformacji pragnę podkreślić, że Ministerstwo podejmuje niezbędne kroki, aby przeciwdziałać dezinformacji, stosowaniu deepfake, czy innym nielegalnym działaniom. W związku z tym zachęcam do zgłaszania dezinformacji przez stronę internetową NASK dedykowaną ku temu: www.zglos-dezinformacje.nask.pl każde zgłoszenie jest weryfikowane i podejmowane są stosowne kroki.

Ad 2) Czy organy władzy państwowej są bezsilne wobec sytuacji w której fałszywe informacje, pomówienia i mowa nienawiści przyczyniają się do eskalacji napięć społecznych, a co za tym idzie wydawania krzywdzących osądów na temat funkcjonowania tak podstawowych instytucji Rzeczypospolitej Polskiej jakimi są organy administracji publicznej, Policja czy Prokuratur? Podkreślenia wymaga również fakt, iż zarówno burmistrz, jak i poseł pełnią funkcje publiczne, stąd wszelkie treści o charakterze dezinformacyjnym są znacznie bardziej dotkliwe, gdyż prowadzą do podważania autorytetów organów władzy publicznej, a w konsekwencji osłabiają zaufanie społeczeństwa do instytucji publicznych. Zwłaszcza że wszystkie wspomniane powyżej profile oraz posty łączy wspólny motyw – wprowadzenie odbiorców w błąd co do sposobu funkcjonowania oraz działalności jednostki samorządu terytorialnego, jej organów oraz innych instytucji publicznych funkcjonujących na jej obszarze. Ponadto, jak już wspomniano, część treści kierowana jest oprócz Pani Burmistrz Prochowic również w stronę Policji i Prokuratury właściwej dla Prochowic oraz Legnicy, sugerując skorumpowanie organów oraz funkcjonowanie w sposób sprzeczny z obowiązującymi przepisami.

Szanowny Panie pragnę podkreślić, że nie każda wypowiedź, czy osąd lub opinia jest dezinformacją, niejednokrotnie za dezinformację uznawana jest krytyka, czy też ostra debata polityczna. Ministerstwo Cyfryzacji jako główny element stanowiący narzędzie zwalczania dezinformacji traktuje budowanie odporności społeczeństwa, umiejętności krytycznego myślenia i promowania sprawdzonych źródeł informacji. Wskazane przez Pana elementy jak krzywdzące osądy co do pracy Administracji Publicznej nie są zjawiskiem nowym i jedynym skutecznym narzędziem ich zwalczania jest przedstawianie informacji prawdziwych. W przypadkach hejtu, naruszenia dóbr osobistych, czy też pomówień istnieją stosowne ścieżki prawne na podstawie Kodeksu Karnego (np. art. 212,216 i 226 Kodeksu Karnego) czy też Cywilnego. Pragnę podkreślić, że Gmina, czy sam Burmistrz jest zobowiązany do obrony autorytetu Urzędu i posiada z pewnością zaplecze prawne, które może podjąć odpowiednie kroki, w przypadku działań ściganych z urzędu powinien zwrócić się w tej kwestii do odpowiednich służb.

Ad 3) Uwzględniając fakt, że sprawa ta ma niezwykle istotny charakter nie tylko na poziomie lokalnym, lecz także bezpieczeństwa informacyjnego oraz jakości debaty publicznej w całym kraju. Weryfikowanie tego rodzaju treści oraz reagowanie na manipulacje już na poziomie lokalnym pozwala na budowanie odporności informacyjnej. Pragnę uzyskać informację jakie działania administracyjne lub inicjatywy legislacyjne

zamierza podjąć kierowany przez Pana resort aby budować odporność informacyjną, która będzie chronić nie tylko poszczególnych obywateli ale przede wszystkim interes publiczny?

Dezinformacja i jej wpływ na sytuację społeczną polityczną oraz gospodarczą jest coraz większy, w związku z czym prowadzone są działania w postaci kampanii medialnych, społecznych i edukacyjnych mające na celu wzmocnienie odporności społeczeństwa na takie działania. Niezależnie od działań o charakterze przeciwdziałającym i wyprzedzającym prowadzone są również działania mające na celu wykrywanie działalności dezinformacyjnej, identyfikację grup za nią odpowiedzialnych, siatek botów a także działalności prowadzonej przez inne państwa czy organizacje zagraniczne mające wpływ na Polską infosferę.

Z naszego doświadczenia wynika, że najistotniejsze jest przeciwdziałanie w formie działań wyprzedzających, demaskowanie nieprawdziwych informacji i weryfikacja informacji oraz krytyczne myślenie (Pre-bunking, debunking, and fact-checking), wraz z promowaniem umiejętności korzystania z mediów, są kluczowymi czynnikami przeciwdziałania dezinformacji. Budowanie szerokiej sieci organizacji i organów reprezentujących różne światopoglądy i środowiska może być ważnym czynnikiem zwiększającym zaufanie do weryfikatorów faktów i blokującym niektóre strategie stosowane obecnie przez złośliwych aktorów. Ministerstwo Cyfryzacji, realizuje wiele działań z zakresu edukacji dotyczących bezpiecznego korzystania z Internetu, skierowanych do dzieci i młodzieży a także dorosłych. Corocznie w zależności od zapotrzebowania realizowane są projekty z zakresu współpracy Ministra Cyfryzacji z organizacjami pozarządowymi, a także zadania realizowane przez podlegającą MC Naukową i Akademicką Sieć Komputerową.

9 stycznia br. Pan Prezydent Karol Nawrocki załatwił ustawę wdrażającą do polskiego prawa przepisy Aktu o Usługach Cyfrowych. W związku z powyższym będziemy kontynuować prace, aby zapewnić obywatelom bezpieczeństwo i ochronę przed Dezinformacją krajową jak i tą spoza granic Polski.

Mając na uwadze rosnące zagrożenia w Polskiej przestrzeni informacyjnej związane z dezinformacją trwają ciągłe prace nad wzmocnieniem zasobów MC przeciwdziałających dezinformacji. Poniżej przedstawiam informacje o zrealizowanych w ubiegłym roku projektach MC które są bezpośrednio związane ze zwalczaniem dezinformacji jak i budowaniem odporności społeczeństwa. Jednocześnie informuję że większość działań ubiegłorocznych będzie kontynuowana, co więcej planujemy kolejne nowe projekty w tym zakresie.

a. Ośłona informacyjna kampanii wyborczej 2025 r.” działania były realizowane w okresie styczeń – październik 2025 r.

Zadanie zlecone Naukowej i Akademickiej Sieci Komputerowej w ramach zadania publicznego realizowała m.in.:

- rozbudowę i utrzymanie przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK-PIB) w roku 2025 strony <http://www.bezpiecznewybory.pl/>. Serwis ten jest skoncentrowany na szkodliwych treściach wyborczych, pełniąc rolę wiarygodnego kanału do wykrywania, weryfikacji informacji. Serwis stanowił miejsce zgłaszania treści szkodliwych do właścicieli mediów społecznościowych oraz umożliwiał publikację artykułów specjalistycznych. Będzie w nim można znaleźć zweryfikowane treści, potwierdzone u źródła informacje na temat procesu wyborczego oraz poradniki i wskazówki.
- Weryfikację treści przesłanych od użytkowników serwisu i obywateli.

- Realizowano regularny monitoring polskojęzycznych mediów społecznościowych w okresie przedwyborczym i w dniu wyborów prezydenckich.
- Przygotowano raporty badawcze z okresu wyborów prezydenckich 2025 r. oraz dodatkowe raporty analityczne obejmujące główne narracje i aktorów zaangażowanych w dezinformację w okresie przedwyborczym.
- Przeprowadzono szkolenia związane z identyfikacją treści dezinformacyjnych dla Komitetów Wyborczych oraz pracowników ambasad Rzeczypospolitej Polskiej zaangażowanych w proces wyborczy.
- Wyprodukowano i wyemitowano krótkie filmy edukacyjne dotyczące zachowań związanych z weryfikacją dezinformacji.

Głównym elementem dotacji był monitoring treści publikowanych w polskiej infosferze a także działania edukacyjne i szkoleniowe.

Projekt był jednym z głównych elementów Parasola Wyborczego.

„Parasol Wyborczy”, uruchomiony w lutym 2025 r. z inicjatywy Ministerstwa Cyfryzacji (MC) we współpracy z Ministerstwem Spraw Wewnętrznych i Administracji (MSWiA), objął trzy kluczowe obszary: ochronę przed zagrożeniami w cyberprzestrzeni, **przeciwdziałanie dezinformacji** oraz edukację i współpracę międzyinstytucjonalną. W realizację tego działania włączyły się: MC, Agencja Bezpieczeństwa Wewnętrznego (ABW), Służba Kontrwywiadu Wojskowego (SKW), Ministerstwo Spraw Zagranicznych (MSZ), Centralny Ośrodek Informatyki (COI), poszczególne CSIRT-y (zespoły reagowania na incydenty bezpieczeństwa komputerowego) oraz Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy (NASK). Połączenie kompetencji tych podmiotów umożliwiło kompleksowe działania zgodnie z wyznaczonymi im ustawowo zakresami zadań.

- b. „Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych i stronach internetowych oraz prace rozwojowe nad budowaniem odporności administracji publicznej oraz społeczeństwa wobec zjawiska dezinformacji poprzez działania naukowe i edukacyjne” działania były realizowane w okresie styczeń – grudzień 2025 r.**

W ramach projektu „Monitoring treści o potencjale dezinformacyjnym w mediach społecznościowych i stronach internetowych oraz prace rozwojowe nad budowaniem odporności administracji publicznej oraz społeczeństwa wobec zjawiska dezinformacji poprzez działania naukowe i edukacyjne” w ramach zadania publicznego zrealizowano m.in.:

- Ciągły monitoring infosfery. W tym Analiza i ocena treści pod kątem dezinformacji. Archiwizacja treści w repozytorium. Zgłaszanie wybranych treści do platform społecznościowych, i odpowiednich służb.
- Analizy dezinformacji, Opracowywanie ilościowe oraz/lub jakościowe treści dezinformacyjnych z uwzględnieniem: FIMI, DIMI, infosfery polskiej, rosyjskiej oraz chińskiej.
- Kontynuowane były badania nad wpływem dezinformacji na społeczeństwo oraz badania na temat predykcji trendów w dezinformacji i polaryzacji społecznej, oraz edukacja interesariuszy z administracji publicznej oraz różnych grup społecznych (w tym dzieci i młodzieży) w zakresie przeciwdziałania dezinformacji.

- c. Jako istotny element przeciwdziałania dezinformacji należy wskazać projekt „Bronić się w necie” realizowany w 2025 r. przez NASK-PIB we współpracy z Ministrem Cyfryzacji oraz Agencją Bezpieczeństwa Wewnętrznego (ABW).**

Był to ogólnopolski konkurs edukacyjny dla uczniów szkół ponadpodstawowych, którego celem było zwiększanie świadomości młodzieży na temat cyberprzemocy – ze szczególnym uwzględnieniem mowy nienawiści i hejtu – a także dezinformacji i radyalizacji.

Uczestnicy – w drużynach składających się z 10 uczniów i nauczyciela – realizowali kursy e-learningowe z testami wiedzy, a następnie przygotowywali własne materiały wideo w formie kampanii społecznych. Nagrodzonych zostało aż 55 drużyn – uczniowie otrzymali smartwatche, nauczyciele elektroniczne notatniki, a szkoły konsole do gier z pełnym wyposażeniem. Gala kończąca projekt i wręczenie nagród zostało przygotowane przez zespół MC w siedzibie KPRM.

d. MC we współpracy z NASK zrealizowało w 2025 roku działania edukacyjne w ramach zadania „Higiena cyfrowa 2025” Zadanie publiczne pn. „Higiena cyfrowa 2025” było realizowane od 14 kwietnia do 31 grudnia 2025 r.

Zakresem przedmiotowym zadania było przygotowanie i przeprowadzenie dla uczniów klas IV-VIII szkół podstawowych zajęć o tematyce cyfrowej higieny oraz bezpieczeństwa w sieci. Zajęcia te przeprowadzone były przez nauczycieli przeszkolonych w ramach realizacji niniejszego zadania. Projekt zakładał realizację działań takich jak:

- promowanie higieny cyfrowej jako elementu zdrowego stylu życia,
- pokazywanie zależności pomiędzy zdrowym i zrównoważonym trybem życia a codziennym samopoczuciem i ogólną kondycją w zakresie korzystania z internetu,
- promowanie postaw poprawiających koncentrację, efektywność, poziom energii i zdrowy sen,
- przekazywanie wiedzy na temat bezpieczeństwa w sieci, m.in. cyberzagrożeń i dezinformacji.

W ramach zadania przygotowany został także film edukacyjny dla rodziców dzieci ze szkół podstawowych.

Długofalowym efektem realizacji projektu będzie wzmocnienie kompetencji cyfrowych wśród uczniów szkół podstawowych, ze szczególnym uwzględnieniem higieny cyfrowej i bezpiecznego korzystania z internetu. Dzięki udziałowi w zajęciach uczniowie nauczyli się dostrzegać różnice pomiędzy światem online i offline, zyskali większą kontrolę nad czasem spędzanym w internecie oraz wykształcili nawyki umożliwiające zrównoważone korzystanie z nowych technologii.

e. Ponadto MC w 2025 roku zleciło do NASK - PIB jeszcze realizację projektu „Szkolenia z zaawansowanych kompetencji cyfrowych dla funkcjonariuszy i pracowników Policji i Państwowej Straży Pożarnej z zakresu sztucznej inteligencji, dezinformacji, cyberbezpieczeństwa, w tym cyberhigieny”

Zadanie było realizowane od 1 sierpnia do 31 grudnia 2025 roku. W ramach zadania NASK-PIB przeprowadził specjalistyczne szkolenia w obszarze sztucznej inteligencji, dezinformacji, cyberbezpieczeństwa, w tym cyberhigieny dla poniższych dla poniższych grup odbiorców:

- Policja: funkcjonariusze pełniący służbę w jednostkach organizacyjnych Policji (służby: kryminalna, śledcza, spraw wewnętrznych, prewencyjne (w tym również wyodrębnione oddziały prewencji), kontrterrorystyczne, wspomagające (w tym również pracowników cywilnych)) na wszystkich szczeblach organizacyjnych;
- Państwowa Straż Pożarna (PSP): funkcjonariusze i pracownicy cywilni pełniący służbę/zatrudnieni w jednostkach organizacyjnych Państwowej Straży Pożarnej wymienionych w art. 8 ustawy z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej¹, zwanej dalej „Ustawą o PSP”.

Program szkoleń był dopasowany do potrzeb szkoleniowych grup docelowych tak aby zapewnić uczestnikom niezbędną wiedzę oraz umiejętności umożliwiające skuteczne przeciwdziałanie incydom dezinformacji oraz cyberbezpieczeństwa. Ponadto w zadaniu przewidziano jeszcze zakup i przekazanie uniwersalnych narzędzi umożliwiających bezpieczne uwierzytelnienie w sieci. Urządzenia te zostały przez NASK-PIB zakupione i przekazane instytucjom objętych szkoleniem.

Wskazane powyżej zadania to jedynie część spośród działań MC w tym zakresie.

Z wyrazami szacunku

Paweł Olszewski

Sekretarz Stanu

/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych