Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.11.2025
Warszawa, 17 lutego 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 17 stycznia br. Posła na Sejm RP Pani Danuty Jazłowieckiej w sprawie zabezpieczenia Polski przed atakami hakerskimi i szerzenia fake newsów ze strony państw niedemokratycznych podczas wyborów prezydenckich (interpelacja nr 7376)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie działania podejmuje Ministerstwo Cyfryzacji w celu ochrony polskiej infrastruktury krytycznej przed cyberatakami, w szczególności ze strony rosyjskich grup hakerskich?

Ministerstwo Cyfryzacji (MC) podejmuje wiele działań mających na celu ochronę polskiej cyberprzestrzeni, zgodnie ze swoją rolą w ramach Krajowego Systemu Cyberbezpieczeństwa, ustanowionego poprzez ustawę o krajowym systemie cyberbezpieczeństwa[1]. W kwestii infrastruktury krytycznej, należy zaznaczyć, że w tym zakresie, zgodnie z ustawą o KSC, wiodący jest zespół reagowania na incydenty bezpieczeństwa komputerowego CSIRT GOV prowadzony przez Agencję Bezpieczeństwa Wewnętrznego (ABW).

Jednocześnie MC (oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, którym jest Minister Cyfryzacji), jako punkt centralny KSC, podejmuje szereg działań wzmacniających cyberbezpieczeństwo Polski, w tym takich, których beneficjentem są też inne instytucje KSC, w tym zespoły reagowania na incydenty bezpieczeństwa komputerowe (CSRIT). Najważniejsze przedsięwzięcia realizowane przez Ministerstwo to:

- Projekt AntyDDoS: MC zapewnia centralnie osłonę przed atakami DDoS dla 76 instytucji, w tym dla Sił Zbrojnych RP i służb specjalnych.
- Bezpieczna łączność dla administracji publicznej: MC zapewnia bezpieczny komunikator na urządzenia służbowe dla administracji publicznej i podmiotów KSC, jak również mobilny system łączności niejawnej SKR-Z.
- System CTI: MC zapewnia centralnie system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) na potrzeby własne i 8 innych instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne na poziomie krajowym.
- System S46: MC zapewnia system IT do wymiany informacji i zgłaszania incydentów w ramach KSC (rozwój systemu i podłączanie nowych użytkowników – 39,7 mln zł z KPO – Krajowy Plan Odbudowy).
- Fundusz Cyberbezpieczeństwa: MC zarządza Funduszem Cyberbezpieczeństwa, który pozwala zapewnić specjalistom ds. cyberbezpieczeństwa w sektorze publicznym wynagrodzenie konkurencyjne z sektorem prywatnym (w 2025 r. 355 mln zł).

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077) (ustawa o KSC)

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

ul. Królewska 27
00-060 Warszawa

- Projekt „Cyberbezpieczny Samorząd”: celem projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Umowy o wsparcie grantowe w ramach projektu, na łączną kwotę blisko 1,5 mld zł zostały podpisane z 2495 jednostkami samorządu terytorialnego (środki FERC - Fundusze Europejskie na Rozwój Cyfrowy). Oznacza to, że wsparcie finansowe na wzmocnienie cyberbezpieczeństwa faktycznie otrzyma prawie 90 % wszystkich samorządów w kraju.
- Cyberbezpieczny Rząd: wsparcie cyberbezpieczeństwa naczelnych i centralnych organów administracji rządowej oraz wojewodów w obszarach kompetencji, technologii i organizacji (350 mln zł z KPO).
- Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa: wsparcie na modernizację i profesjonalizację zespołów policji, które będą wspierać zaatakowane podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych (37,5 mln zł z KPO).
- Utworzenie i rozwój sektorowych zespołów CSIRT (66 mln zł z KPO).
- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa, a także stacjonarne szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie w ramach projektu SecureV.

Poza tym, w celu należytej koordynacji bieżącego zarządzania cyberbezpieczeństwem MC i Rządowe Centrum Cyberbezpieczeństwa (RCB) organizują spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). Funkcjonowanie PCOC umożliwia szybką wymianę informacji oraz reagowania na pojawiające się incydenty. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa. W procedowanej nowelizacji ustawy o KSC planowane jest sformalizowanie działania PCOC (faktycznie funkcjonującego od 2022 r.). Planowane jest dalsze wzmacnianie PCOC i jego instytucjonalizacja.

Z kolei współpraca na poziomie strategiczno-politycznym realizowana jest w ramach Kolegium do Spraw Cyberbezpieczeństwa. Z upoważnienia Prezesa Rady Ministrów Kolegium przewodniczy Wicepremier i Minister Cyfryzacji, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa. Obsługę Kolegium zapewnia Ministerstwo Cyfryzacji.

Ministerstwo Cyfryzacji opracowało także projekt nowelizacji ustawy KSC, wdrażający w Polsce dyrektywę NIS 2, który jest obecnie procedowany w rządzie. Wejście w życie tych przepisów znacząco przemodeluje KSC oraz podniesienie poziom cyberbezpieczeństwa w Polsce.

Ponadto, Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydaje rekomendacje i komunikaty, których wdrożenie przez podmioty KSC (w tym instytucje publiczne) pozwala minimalizować ryzyka związane z identyfikowanymi podatnościami oraz kampaniami w cyberprzestrzeni.

Ważne są także działania innych instytucji, takie jak:

- ARAKIS GOV: ABW prowadzi system wczesnego ostrzegania o zagrożeniach w sieci Internet, który powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej.
- ARTEMIS: CSIRT NASK rozwija narzędzie Artemis, służące do wykrywania najczęściej występujących podatności i błędów konfiguracyjnych obecnych w

ramach usług sieciowych, a także przekazuje osobom odpowiedzialnym za dany system informacje o znalezionych podatnościach i błędnych konfiguracjach.

Natomiast w kontekście ujętych w tytule interpelacji zagrożeń cyberbezpieczeństwa w odniesieniu do wyborów prezydenckich, oprócz opisanych powyżej działań, które również mają zastosowanie w tym przypadku, należy wyjaśnić, że instytucją wiodącą w zakresie zapewniania cyberbezpieczeństwa wyborów jest ABW, zgodnie z jej ustawowymi kompetencjami określonymi w ustawie o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu oraz ustawie o krajowym systemie cyberbezpieczeństwa (zadania zespołu CSIRT GOV prowadzonego przez ABW). MC i Pełnomocnik Rządu ds. Cyberbezpieczeństwa uczestniczy w działaniach związanych zapewnieniem cyberbezpieczeństwa wyborów, w tym w ramach PCOC.

Ad 2) Czy w ramach polityki cyberbezpieczeństwa Polski przewidziane są działania prewencyjne, takie jak regularne testy systemów IT administracji publicznej oraz państwowych przedsiębiorstw?

Należy zaznaczyć, że za bezpieczeństwo systemów teleinformatycznych i świadczonych za ich pomocą usług (w tym np. poprzez testy) odpowiada właściciel danego systemu. Musi on spełniać wymagania i obowiązki wynikające z przepisów ustawy o KSC oraz innych przepisów prawa (np. dotyczących ochrony danych osobowych, ochrony informacji niejawnych, krajowych ram interoperacyjności, czy też przepisów obowiązujących w poszczególnych sektorach, takich jak sektor bankowości). Wdrożenie w Polsce dyrektywy NIS 2 poprzez nowelizację ustawy o KSC znacząco rozszerzy obowiązki podmiotów KSC związane z zapewnianiem odpowiedniego poziomu cyberbezpieczeństwa.

Ponadto, do podnoszenia odporności systemów teleinformatycznych oraz niektórych przedsiębiorstw (m.in. operatorów usług kluczowych i operatorów infrastruktury krytycznej) wykorzystywane są inicjatywy wymienione w odpowiedzi na pytanie nr 1.

W zakresie bezpieczeństwa państwowych systemów i rejestrów oraz cyfrowych usług publicznych kluczowe są działania Centralnego Ośrodka Informatyki (COI), jednostki nadzorowanej przez Ministra Cyfryzacji. W COI, które jest odpowiedzialne za rozwój i utrzymanie wielu rejestrów państwowych i usług cyfrowych (np. mObywatel), funkcjonuje zespół Security Operation Center (SOC) monitorujący w trybie 24/7 bezpieczeństwo systemów. Zespół ten ściśle współpracuje z CSIRT GOV i CSIRT NASK oraz stale podnosi zdolności do monitorowania i reagowania na incydenty poprzez wdrażanie nowych rozwiązań technologicznych oraz systemowych. Utrzymywane systemy przechodzą cykliczne testy ciągłości działania, mające na celu zweryfikowanie prawidłowości funkcjonowania systemu w przypadku wystąpienia sytuacji kryzysowej np. awarii, a także weryfikacji i doskonalenia działań poszczególnych zespołów. Obecnie we wszystkie działania związane z budową i rozwojem utrzymywanych rozwiązań włączani są Architekci Bezpieczeństwa, tak aby zminimalizować możliwość wystąpienia słabości w tworzonym oprogramowaniu. Stanowi to element podejścia shift-left, którego celem jest włączenie w proces wytwórczy na jak najwcześniejszym etapie działań związanych z bezpieczeństwem.

Należy również zauważyć, że od lutego 2022 r. na terytorium RP obowiązywał trzeci stopień alarmowy CHARLIE-CRP. Zgodnie z ustawą o działaniach antyterrorystycznych stopnie te są wprowadzane przez premiera w przypadku zagrożenia o charakterze terrorystycznym dotyczącego systemów teleinformatycznych administracji publicznej lub infrastruktury krytycznej. Od 1 marca 2024 r. obowiązuje stopień alarmowy BRAVO-CRP. Obowiązywanie stopni alarmowych wiąże się z obowiązkiem wdrożenia odpowiednich działań w administracji publicznej i u operatorów infrastruktury krytycznej, które są określone w rozporządzeniu Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP.

Ad 3) Czy Polska posiada kompleksową strategię walki z dezinformacją i fake newsami, w tym mechanizmy szybkiego reagowania na szerzenie fałszywych informacji w przestrzeni publicznej i mediach społecznościowych?

Polska nie posiada wyodrębnionego dokumentu – strategii walki z dezinformacją. Obecnie istnieje mnogość dokumentów w których poświęcono wiele miejsca kwestii dezinformacji - warto wskazać kilka inicjatyw, w tym zakresie:

- "Kodeks dobrych praktyk" w zakresie dezinformacji – opracowany przez jedenaście organizacji i instytucji, koncentruje się na przeciwdziałaniu rozpowszechnianiu nieprawdziwych informacji. Dokument zawiera rekomendacje w zakresie fact-checkingu, zgłaszania i blokowania treści dezinformacyjnych oraz edukowania społeczeństwa w zakresie odróżniania informacji prawdziwych od fałszywych.
- Raport "Przeciwdziałanie dezinformacji w Polsce" – przygotowany przez Fundację Security Forum, zawiera ponad 60 rekomendacji dotyczących przeciwdziałania dezinformacji w Polsce. Zaproponowano w nim rozwiązania systemowe, takie jak korygowanie nieprawdziwych informacji, wzmacnianie odporności społecznej oraz przeciwdziałanie społecznym skutkom dezinformacji.

Powyższe dokumenty są inicjatywami sektora rządowego i pozarządowego.

Obecnie Ministerstwo Cyfryzacji pracuje nad dokumentem strategicznym w dziedzinie informatyzacji państwa, zwanym dalej "Strategią Cyfryzacji", przedstawiającym spójną i horyzontalną wizję transformacji cyfrowej Polski. W Strategii Cyfryzacji zostały wyznaczone cele w najważniejszych obszarach cyfryzacji, w tym również w obszarach koncentrujących się na obywatelach, ich jakości życia, rozwoju i prawach w przestrzeni cyfrowej. Jednym z priorytetów jest stworzenie bezpiecznej przestrzeni cyfrowej, czyli zapewnienie praktycznej realizacji praw obywateli w sferze cyfrowej i przeciwdziałanie dezinformacji. Ministerstwo Cyfryzacji jako działania służące do realizacji powyższego celu wskazało m.in.:

- Ustalenie organu odpowiedzialnego za nadzorowanie i integrowanie działań różnych podmiotów zajmujących się przeciwdziałaniem dezinformacji,
- Opracowanie jednolitych lub zbliżonych procedur i standardów operacyjnych stosowanych przez jednostki zajmujące się przeciwdziałaniem dezinformacji,
- Realizacja kampanii informacyjnych i społecznych na temat dezinformacji i odpowiedzialnego korzystania z mediów,
- Prowadzenie dedykowanych kampanii informacyjnych w związku z kluczowymi wydarzeniami.

Projekt Strategii Cyfryzacji został przedstawiony do konsultacji społecznych, w ramach których Ministerstwo Cyfryzacji otrzymało stanowiska i uwagi. Obecnie trwa ich szczegółowa analiza i uzupełnianie projektu, po zakończeniu którego opublikowane zostanie podsumowanie procesu.

Ad 4) Czy Ministerstwo Cyfryzacji współpracuje z międzynarodowymi instytucjami, takimi jak ENISA (Europejska Agencja ds. Cyberbezpieczeństwa), NATO CCDCOE (Centrum Doskonalenia Obrony Cybernetycznej NATO) lub platformami technologicznymi, w celu wymiany informacji o zagrożeniach i opracowywania wspólnych standardów obrony?

Tak, MC współpracuje w zakresie cyberbezpieczeństwa z organizacjami międzynarodowymi i ich agendami, w szczególności z ENISA. Przy czym w zakresie

współpracy z NATO CCDCOE wiodące jest Ministerstwo Obrony Narodowej, z uwagi na to, że jest to organizacja działająca w obszarze obronności.

MC współpracuje także z firmami technologicznymi w ramach Programy Współpracy w Cyberbezpieczeństwie (PWCyber)[2].

Ad 5) Jakie środki finansowe są przeznaczane na rozwój polskich zasobów cyberbezpieczeństwa, w tym szkolenia specjalistów, rozwój narzędzi do ochrony danych oraz budowę zespołów szybkiego reagowania na incydenty cybernetyczne?

Zgodnie z ustawą o KSC w Polsce funkcjonują trzy zespoły CSRIT poziomu krajowego:

1) CSIRT GOV – prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) CSIRT MON – prowadzony przez Ministra Obrony Narodowej;
3) CSIRT NASK – prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK-PIB).

MC jako instytucja nadzorująca NASK-PIB udziela corocznie dotacji dla NASK-PIB na funkcjonowanie CSIRT NASK. W 2024 r. wyniosła ona 34 000 000,00 zł, a w 2025 r., zgodnie z projektem umowy dotacyjnej, planowane jest przeznaczenie na ten cel 39 186 000,00 zł.

Ponadto, MC realizuje projekt „Centrum Cyberbezpieczeństwa NASK" o wartości 310 mln zł (z FERC), którego celem jest wzmocnienie KSC poprzez utworzenie przy NASK Centrum Cyberbezpieczeństwa, na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria. Na projekt ten składają się 3 następujące powiązane ze sobą podzadania: utworzenie obiektu CCN; utworzenie 7 specjalistycznych centrów, ośrodków i laboratoriów; rozbudowa infrastruktury NASK-PIB działającej na rzecz CSIRT NASK.

Poza tym, MC ściśle współpracuje z zespołami CSIRT, wspiera je i realizuje inwestycje podnoszące ich potencjał, w tym poprzez inicjatywy wymienione w odpowiedzi na pytanie nr 1 (których beneficjentami są także zespoły CSIRT: projekt AntyDDoS, bezpieczna łączność, system CTI, system S46, Fundusz Cyberbezpieczeństwa, PCOC).

Poza tym, procedowana nowelizacja ustawy o KSC przewiduje utworzenie sektorowych zespołów CSIRT, za których powołanie będą odpowiedzialne organy właściwe do spraw cyberbezpieczeństwa (poszczególne resorty właściwe w danych sektorach, w tym MC). Na realizację inwestycji przygotowanej przez MC, związanej z utworzeniem i rozwojem sektorowych zespołów CSIRT przeznaczone zostanie 66 mln zł z KPO.

Ad 6) Czy Ministerstwo prowadzi lub planuje prowadzić kampanie edukacyjne skierowane do społeczeństwa, mające na celu podnoszenie świadomości na temat cyberzagrożeń, fake newsów oraz zasad ochrony danych w sieci?

Jednym z kluczowych zadań Ministerstwa jest promowanie pozytywnych postaw w interakcjach w środowisku cyfrowym oraz walka z występującymi w nim negatywnymi zjawiskami, w tym dezinformacją, oraz prowadzenie innych działań mających na celu zwiększanie poziomu kompetencji cyfrowych w społeczeństwie.

Analogicznie jak to miało miejsce w 2024 r. Ministerstwo Cyfryzacji planuje przeprowadzenie kampanii społecznych mających na celu uświadomienie obywatelom jakie zagrożenia niesie ze sobą dezinformacja. Planujemy również wspólnie z Naukową i Akademicką Siecią Komputerową realizację zwalczania dezinformacji poprzez m.in. uświadamianie ogółu społeczeństwa jak i konkretnych grup osób, np. w okresie

[2] https://www.gov.pl/web/cyfryzacja/program-wspolpracy-w-cyberbezpieczenstwie-pwcyber

wyborczym planowane są szkolenia dla komitetów wyborczych, członków komisji, kandydatów.

Ministerstwo Cyfryzacji prowadzi szereg działań prewencyjno-edukacyjnych skierowanych do społeczeństwa, w szczególności:

- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa: od 2020 r. prowadzone są bezpłatne szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Dotychczas przeprowadzono 123 szkolenia, w których uczestniczyło ponad 66 tys. osób, a w tym:
  - szkolenia dla kadr podmiotów publicznych;
  - szkolenia dla operatorów usług kluczowych;
  - szkolenia dla użytkowników Systemów Rejestrów Państwowych;
  - szkolenia dla podmiotów publicznych wykonujących działalność leczniczą.
- Szkolenie e-learningowe: w 2023 r. uruchomione zostało szkolenie e-learningowe pn. „Podstawowe zasady cyberbezpieczeństwa oraz zasady bezpieczeństwa stacji roboczych SRP", które jest dostępne na platformie https://szkolenia.obywatel.gov.pl/. Od 2023 r. szkolenie odbyło ponad 1700 pracowników administracji publicznej.
- Szkolenie z cyberhigieny na platformie szkolenia.gov.pl: w I kwartale 2025 r. na rządowym portalu szkolenia.gov.pl uruchomione zostanie szkolenie z zakresu cyberbezpieczeństwa. Szkolenie będzie dostępne dla każdego zainteresowanego po zalogowaniu na platformę szkolenia.gov.pl (z pomocą profilu zaufanego). Szkolenie jest e-learningowym kursem dotyczącym podstaw cyberbezpieczeństwa, stworzonym z myślą o wszystkich obywatelach pragnących zwiększyć swoją wiedzę na temat ochrony danych osobowych i prywatności w sieci.
- Projekty SecureV: od 2021 r. prowadzone są działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa m.in. dla najważniejszych osób w państwie (projekty SecureV). Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej. Jednak z uwagi na dynamiczną sytuację w cyberprzestrzeni oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców. W 2023 r. szkoleniami objęci byli: parlamentarzyści, kadra kierownicza administracji rządowej (centralnej i terenowej) i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej. Tylko w 2024 r. przeszkolono blisko 5 tys. osób.
- Projekt Cyberlekcje: od 2021 r. Ministerstwo Cyfryzacji wspólnie z NASK-PIB realizuje projekt adresowany do nauczycieli i pedagogów, chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w Internecie. W ramach projektu Cyberlekcje powstało 18 gotowych scenariuszy zajęć lekcyjnych o cyberbezpieczeństwie skierowanych do różnych grup wiekowych uczniów w szkołach podstawowych i ponadpodstawowych. W ramach projektu powstały również dodatkowe materiały, jak: infografiki, prezentacje, animacje oraz filmy z ekspertami, które wraz z scenariuszami są udostępnione dla wszystkich zainteresowanych w powszechnie dostępnej bazie wiedzy cyberbezpieczeństwa na portalu gov.pl w zakładce CyberEdukacja, a także na Zintegrowanej Platformie Edukacyjnej, narzędziu rekomendowanym przez Ministerstwo Edukacji Narodowej. W 2024 r. zrealizowany został pilotaż w ramach którego przeprowadzono m.in. stacjonarne szkolenia dla kadry pedagogicznej.
- Konkurs CyberWizards 2024 – International Cyber Camp: Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej zorganizowało nabór do CyberWizards International Camp. Nagrodą był cyberobóz w Estonii dla zwycięskiej drużyny. Wysłanie do Estonii polskiej drużyny dziewcząt stanowi jeden z wielu

elementów promujących od najmłodszych lat karierę kobiet w branży cyberbezpieczeństwa.

Należy jednocześnie zaznaczyć, że działania w zakresie edukacji o bezpiecznym korzystaniu z narzędzi cyfrowych (element obowiązującej podstawy programowej nauczania w szkole podstawowej i ponadpodstawowej) realizuje Ministerstwo Edukacji Narodowej, jako właściwe w tym zakresie.

Ad 7) Czy polskie regulacje prawne są dostosowane do przeciwdziałania nowoczesnym formom cyberprzestępczości i dezinformacji, w tym w kontekście współpracy z platformami społecznościowymi i dostawcami usług internetowych?

W kontekście tego pytania należy zwrócić uwagę, że Ministerstwo Cyfryzacji prowadzi prace nad projektem ustawy o zmianie ustawy o świadczeniu usług drogą elektroniczną oraz niektórych innych ustaw[3], stanowiącym wdrożenie 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). W projekcie tym zawarte są przepisy które są wymagane do wdrożenia w prawie krajowym tj. głównie wskazanie regulatorów odpowiedzialnych w Polsce za nadzór i egzekwowanie przepisów rozporządzenia oraz dopracowanie procedur krajowych. Ustawa wdrażająca DSA do polskiego porządku prawnego znajduje się obecnie na etapie rozpatrywania przez Stały Komitet Rady Ministrów.

Akt o usługach cyfrowych (DSA) obowiązuje w pełni od 17 lutego 2024 r. Jednym z głównych celów uchwalenia DSA jest zapewnienie „(...) bezpiecznego, przewidywalnego i budzącego zaufanie środowiska internetowego (...)" (art. 1 ust. 1 DSA), w zakresie tego zadania mieści się również zwalczanie dezinformacji. Świadczy o tym użycie słowa dezinformacja w kilku motywach DSA. Jednocześnie jednak dezinformacja nie została zdefiniowana w tym akcie prawnym. Tymczasem mówiąc o dezinformacji trzeba podkreślić rozróżnienie w DSA w podejściu do zwalczania treści szkodliwych i treści nielegalnych:

- obowiązek zwalczania treści nielegalnych dotyczy wszystkich pośredników internetowych, (przy czym nielegalne treści zgodnie z DSA to informacje, które same w sobie lub przez odniesienie do działań, takich jak sprzedaż produktów lub świadczenie usług, nie są zgodne ani z prawem Unii Europejskiej, ani z prawem jakiegokolwiek państwa członkowskiego, które przestrzega prawa Unii, niezależnie od konkretnego przedmiotu lub charakteru tego prawa),
- w przypadku treści szkodliwych w DSA nałożono szczególne obowiązki w sprawie identyfikowania i ograniczania ryzyka związanego z rozpowszechnianiem tego typu treści tylko na wybraną tylko kategorię pośredników internetowych, tj. „bardzo duże platformy internetowe", „bardzo duże wyszukiwarki internetowe".

Należy zwrócić uwagę, że zjawisko dezinformacji nie ma ustalonej, wiążącej definicji w polskim prawie. Do tego w kontekście rozpowszechniania nieprawdziwych lub wprowadzających w błąd informacji mogą w praktyce okazać się bardzo trudne do wykazania i udowodnienia. Z tego względu przeciwdziałanie dezinformacji należy raczej rozpatrywać w kontekście przeciwdziałania narracjom o charakterze dezinformacyjnych, czy też działań współregulacyjnych podejmowanych na poziomie UE.

W przypadku praktycznego przeciwdziałania dezinformacji przykładem mogą być zadania podejmowane przez NASK takie jak utrzymanie i rozwój serwisu www.bezpiecznewybory.pl na potrzeby obywateli oraz podmiotów realizujących zadania publiczne. Dzięki udostępnieniu danych z monitoringu, obszernych analiz oraz tekstów

[3] numer w wykazie prac legislacyjnych Rady Ministrów - UC21

eksperckich, w ramach serwisu www.bezpiecznewybory.pl wyborcy oraz instytucje mogą znaleźć rzetelne źródło wiedzy na temat wykrywania oraz przeciwdziałania dezinformacji w trakcie wyborów. Na stronie dostępny jest także formularz do zgłaszania treści dezinformacyjnych do oceny przez Dział Przeciwdziałania Dezinformacji.

W odniesieniu do działań współregulacyjnych podejmowanych na poziomie unijnym, należy wskazać na Wzmocniony kodeks postępowania w zakresie zwalczania dezinformacji z 16 czerwca 2022 r. Kodeks, w rozumieniu DSA będzie również wykorzystywany przez duże platformy internetowe do ograniczenia ryzyka związanego z rozpowszechnianiem dezinformacji.

Z wyrazami szacunku
Paweł Olszewski
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