



# Ministerstwo Cyfryzacji

Sekretarz Stanu  
Paweł Olszewski

BM.WP.057.98.2026  
Warszawa, 20 lipca 2026 r.

**Szanowny Pan  
Włodzimierz Czarzasty  
Marszałek Sejmu RP**

Dot. pisma z 26 maja br. Pośła na Sejm RP Pana Wiesława Krajewskiego w sprawie  
narastającego wykluczenia cyfrowego obywateli (interpelacja nr 17358)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

## **Ad 1) Ilu obywateli w Polsce zagrożonych jest wykluczeniem cyfrowym?**

Teza sformułowana w tytule interpelacji pt. „Interpelacja w sprawie narastającego wykluczenia cyfrowego obywateli” nie znajduje potwierdzenia w dostępnych danych, ponieważ poziom wykluczenia cyfrowego w Polsce nie wykazuje tendencji wzrostowej, lecz ulega stopniowemu ograniczaniu.

Zmiany wartości przedstawionych poniżej wskaźników na przestrzeni ostatnich lat dobitnie świadczą o malejącej skali wykluczenia cyfrowego:

### **a) Dostęp do internetu w Polsce**

W 2021 r. 92% gospodarstw domowych w Polsce miało dostęp do internetu, co lokowało Polskę na 12 miejscu wśród krajów europejskich, a w 2025 r. wskaźnik ten osiągnął wartość 96% dając Polsce 9. pozycję w Unii Europejskiej, gdzie średnia wyniosła 95%. Bardzo istotny dla integracji cyfrowej jest fakt, że różnice w dostępie do internetu między miastami a wsią w Polsce niemal zatarły się, ponieważ 96% wiejskich gospodarstw domowych i 97% miejskich dysponowało internetem w 2025 r.

W Polsce niemal wszystkie gospodarstwa domowe z dostępem do internetu korzystały z łączny szerokopasmowych (95% w 2025 r. i 92% gospodarstw domowych w 2021 r.)

### **b) Wykluczenie cyfrowe - niekorzystanie z internetu**

Skala pierwotnego wykluczenia cyfrowego w Polsce, rozumianego jako odsetek populacji nigdy niekorzystającej z internetu, ukształtowała się na poziomie 11% w 2021 r. i 8% w 2025 r.

### **c) Kompetencyjne wykluczenie cyfrowe**

W 2025 r. odsetek osób posiadających co najmniej podstawowe umiejętności cyfrowe w Polsce wyniósł 50%, o 7 p.p. więcej niż w 2021 r., co pozwoliło Polsce poprawić swoją pozycję wśród państw członkowskich UE o dwa miejsca i zająć 23. pozycję.

Ponadto, należy zaznaczyć, że zgodnie z właściwością minister właściwy do spraw informatyzacji nadzoruje także prawidłowe wdrażanie przez podmioty publiczne wymogów dostępności cyfrowej stron internetowych i aplikacji mobilnych. Brak dostępności cyfrowej naraża osoby z niepełnosprawnościami oraz innych użytkowników, w tym osoby starsze na wykluczenie cyfrowe spowodowane niemożnością korzystania przez te osoby z treści cyfrowych, które nie spełniają wymogów dostępności cyfrowej. Liczbę osób korzystających z dostępności cyfrowej szacujemy na 11 mln, są to dane z GUS za rok 2024. Zatem ponad 11 mln osób może być narażonych na wykluczenie cyfrowe, gdy strony internetowe i aplikacje mobilne nie będą spełniać wymogów dostępności

cyfrowej określonych w załączniku do ustawy z 4 kwietnia 2019 r. o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych.

## **Ad 2) Czy rząd posiada aktualny program przeciwdziałania wykluczeniu cyfrowemu?**

Przedstawione dane wskazują, że infrastrukturalny wymiar wykluczenia cyfrowego w Polsce ma obecnie charakter ograniczony i nie stanowi głównej bariery w dostępie obywateli do usług cyfrowych. Jednocześnie należy podkreślić, że istotnym wyzwaniem pozostaje wykluczenie kompetencyjne, które dotyczy znaczącej części społeczeństwa, w szczególności osób o niższych umiejętnościach cyfrowych.

W odpowiedzi na ten problem podejmowane są działania o charakterze systemowym, w tym przyjęcie przez Radę Ministrów Programu Rozwoju Kompetencji Cyfrowych, ukierunkowanego na podnoszenie kompetencji cyfrowych obywateli. Program ten stanowi istotny element polityki publicznej w perspektywie do 2030 r. w zakresie przeciwdziałania wykluczeniu cyfrowemu. Obecnie trwa nowelizacja Programu, której celem jest jeszcze większa intensyfikacja działań pozwalających na osiągnięcie w 2030 r. następujących celów:

- 80% mieszkańców Polski będzie posiadać co najmniej podstawowe kompetencje cyfrowe;
- 40% mieszkańców Polski będzie posiadać ponadpodstawowe kompetencje cyfrowe;
- 6% pracujących będą stanowić specjaliści ICT;
- 29% specjalistów ICT będą stanowić kobiety;
- na szczeblu administracji rządowej funkcjonować będzie ugruntowany i sprawdzony mechanizm koordynacji i monitorowania działań wspierających rozwój kompetencji cyfrowych, który bazuje na cyklicznie aktualizowanej diagnozie potrzeb społeczeństwa, biorący pod uwagę najnowsze trendy technologiczne i gospodarcze.

Ponadto, poza ww. działaniami MC podejmuje inne działania, które wprost wynikają z ustawy o dostępności cyfrowej i m. in. polegają na corocznym monitoringu stron internetowych i aplikacji mobilnych podmiotów publicznych znajdujących się w wykazie stron internetowych prowadzonym przez Ministra Cyfryzacji. Wyniki monitoringu są opracowywane w corocznych sprawozdaniach z wyników monitorowania publikowanych w Biuletynie Informacji Publicznej Ministra Cyfryzacji. Ponadto podmioty publiczne, których strony internetowe lub aplikacje były monitorowane są informowane o wynikach monitoringu ze wskazaniem usunięcia błędów dostępności. Minister Cyfryzacji prowadzi również działania informacyjno-edukacyjne oraz rządowy portal o dostępności cyfrowej.

Minister Cyfryzacji działa również jako organ nadzoru rynku w zakresie usług handlu elektronicznego zgodnie z ustawą z 26 kwietnia 2024 r. o zapewnianiu spełniania wymogów dostępności niektórych produktów i usług przez podmioty gospodarcze.

Podkreślić należy również, że w uchwale nr 130 Rady Ministrów z dnia 9 czerwca 2026 r. w sprawie przyjęcia strategii dotyczącej informatyzacji państwa<sup>1</sup>, tj. Strategii Cyfryzacji Państwa, opracowanej przez Ministerstwo Cyfryzacji we współpracy z członkami Rady Ministrów, wskazano kierunki cyfrowej transformacji państwa, w tym również w obszarze kompetencji cyfrowych, które mają fundamentalne znaczenie dla rozwoju sfery cyfrowej w państwie.

Skuteczna cyfryzacja państwa, obejmująca rozwój usług cyfrowych oraz transformację procesów administracyjnych, wymaga równoległego i systemowego rozwoju kompetencji

---

<sup>1</sup> Monitor Polski 2026 r. poz. 620

cyfrowych, obejmującego obywateli, ale też pracowników administracji publicznej na wszystkich szczeblach.

W związku z tym, w Strategii przewidziano szereg działań, mających na celu przeciwdziałanie wykluczeniu cyfrowemu, m.in.:

- 1) Zwiększenie umiejętności cyfrowych wśród polskiego społeczeństwa, m.in.:
  - Zapewnienie osobom dorosłym możliwości rozwoju umiejętności cyfrowych w tworzonych Klubach Rozwoju Cyfrowego;
  - Inicjowanie działań wspierających osoby z niepełnosprawnościami i szczególnymi potrzebami (np. wsparcie finansowe w zakupie sprzętu, organizowanie szkoleń);
  - Budowanie świadomości w zakresie bezpiecznego poruszania się w świecie cyfrowym oraz systemowe przeciwdziałanie dezinformacji, rozwijanie kompetencji krytycznego myślenia, umiejętności weryfikacji informacji i korzystania z mediów na wszystkich poziomach kształcenia.
- 2) Zapewnienie efektywnej i wysokiej jakości edukację cyfrową na wszystkich poziomach kształcenia, m.in.:
  - Podniesienie jakości kształtowania kompetencji cyfrowych młodego pokolenia przez rozwój dydaktyki cyfrowej oraz dostosowanie podstawy programowej do postępu technologicznego;
  - Wykorzystanie technologii cyfrowych w szkołach do podnoszenia jakości kształcenia;
  - Wprowadzenie do podstawy nauczania na wszystkich poziomach kształcenia oraz programów kształcenia i doszkalania kadry dydaktycznej (rozwijania kompetencji miękkich związanych ze sferą cyfrową oraz kształtowania umiejętności bezpiecznego korzystania z e-usług publicznych i prywatnych).
- 3) Zwiększenie kompetencji cyfrowych wśród pracowników administracji publicznej, w tym JST, np.:
  - Pracownikom administracji publicznej, w tym samorządowym, dostępu do wysokiej jakości szkoleń, warsztatów praktycznych oraz pakietów kursów e-learningowych;
  - Opracowanie i wdrożenie systemu podnoszenia poziomu kompetencji cyfrowych pracowników samorządowych;
  - Wsparcie samorządów w tworzeniu lokalnych, regionalnych lub ponadregionalnych hubów usług i kompetencji cyfrowych.

Jednocześnie, warto zaznaczyć, że Ministerstwo Cyfryzacji stoi na stanowisku, że tworzenie nowych e-usług publicznych czy podnoszenie użyteczności już istniejących nie powinno pozbawiać obywateli możliwości załatwienia sprawy w sposób tradycyjny (w urzędzie). Skorzystanie z elektronicznych usług publicznych powinno mieć charakter dobrowolny i to obywatel powinien mieć możliwość wyboru, czy chce załatwić sprawę cyfrowo czy tradycyjnie.

### **Ad 3) Jakie działania podejmowane są wobec seniorów mających problemy z korzystaniem z usług cyfrowych?**

Wymieniony wyżej Program Rozwoju Kompetencji Cyfrowych zawiera następujące działania dedykowane osobom stawiającym pierwsze kroki w świecie cyfrowym, w tym seniorom:

- 1) Rozwój kompetencji cyfrowych osób wykluczonych, z niepełnosprawnościami lub z niskim poziomem kompetencji cyfrowych.
- 2) Systemowe wsparcie edukacji cyfrowej dorosłych użytkowników ICT – Kluby Rozwoju Cyfrowego.
- 3) Kampanie edukacyjno-informacyjne na rzecz rozwoju kompetencji cyfrowych.
- 4) Szkolenia dla obywateli z kompetencji cyfrowych.
- 5) Szkoła Międzypokoleniowa, w której uczniowie i nauczyciele szkół podstawowych i ponadpodstawowych wspierają rozwój kompetencji cyfrowych seniorów.
- 6) eFajfy, obejmujące organizację i przeprowadzenie bezpłatnych szkoleń z zakresu bezpieczeństwa w sieci i korzystania z e-usług dla seniorów, którzy przebywają w sanatoriach.

Odnosząc się natomiast do Strategii Cyfryzacji Państwa – jej głównym celem jest poprawa jakości życia obywateli, dzięki cyfryzacji. Strategia wyznacza więc cele i działania, których realizacja ułatwi użytkownikom m.in. komunikację z organami administracji publicznej (tj. dalszy rozwój e-usług – prostszych, bardziej intuicyjnych i dostępnych, uproszczenie procedur administracyjnych, czy wprowadzenie domyślności cyfrowej).

Dzięki modernizacji istniejących i wdrożeniu nowych rozwiązań, zaprojektowanych w Strategii, administracja publiczna będzie jeszcze bardziej przyjazna, dostępna i dopasowana do potrzeb różnych grup użytkowników, w tym osób ze szczególnymi potrzebami czy osób starszych.

W Strategii przewidziano działania mające na celu uproszczenie korzystania z elektronicznych usług publicznych, m.in.:

- Osiągnięcie pełnej zgodności e-usług z krajowymi i europejskimi wymaganiami dostępności cyfrowej oraz prowadzenie bieżących audytów obecnie działających usług pod kątem dostępności, dostosowanie istniejących rozwiązań i obowiązkowe wdrażanie standardów dostępności cyfrowej w nowych projektach;
- Opracowanie standardów UX/UI dla wszystkich e-usług oraz bieżące testowanie ich z różnorodnymi grupami użytkowników, na wszystkich etapach procesu wytwórczego oraz umożliwienie wymiany dobrych praktyk dotyczących projektowania doświadczeń użytkowników wśród jednostek administracji publicznej;
- Inicjowanie działań wspierających osoby z niepełnosprawnościami i szczególnymi potrzebami, obejmujących: wsparcie finansowe w zakupie sprzętu niezbędnego do nabycia kompetencji cyfrowych; organizowanie przeznaczonych dla nich szkoleń; wsparcie organizacji non-profit w realizacji działań na rzecz podnoszenia kompetencji cyfrowych wśród osób z niepełnosprawnościami i szczególnymi potrzebami.

Jednocześnie w Strategii wskazano, że państwo powinno zapewnić dobrowolność korzystania z rozwiązań cyfrowych, związanych z komunikacją z administracją publiczną oraz realizacją usług. Oznacza to, że użytkownik nadal powinien mieć możliwość załatwienia spraw w urzędzie tradycyjnie, a nie tylko cyfrowo.

#### **Ad 4) Czy analizowano skutki likwidacji placówek bankowych i punktów obsługi stacjonarnej?**

Przedmiotowa kwestia pozostaje poza zakresem właściwości Ministerstwa Cyfryzacji.

#### **Ad 5) Jakie środki przeznaczono na edukację cyfrową obywateli?**

Koszt realizacji Programu Rozwoju Kompetencji Cyfrowych, został oszacowany na poziomie 2 789 mln zł w perspektywie do 2030 r. W wyniku jego aktualizacji oraz

rozszerzenia zakresu działań przewiduje się wzrost łącznych nakładów na rozwój kompetencji cyfrowych do kwoty 3,98 mld zł.

W zakresie dostępności cyfrowej należy wskazać, że Ministerstwo Cyfryzacji realizuje czteroletni projekt finansowany ze środków FERS „Systemowe kształcenie specjalistek i specjalistów dostępności cyfrowej”. W ramach realizowanego projektu przeszkolimy 2200 osób. Zwiększy się tym samym liczba ekspertów dostępności cyfrowej, co będzie miało wpływ na poprawę dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych i gospodarczych.

Projekt realizowany jest w ramach programu Fundusze Europejskie dla Rozwoju Społecznego 2021-2027, współfinansowanego ze środków Europejskiego Funduszu Społecznego Plus, wartość projektu – 58 259 564,00 zł, w tym wkład z Funduszy Europejskich – 48 075 792,21 zł.

#### **Ad 6) Jakie działania podejmowane są wobec rosnącej liczby cyberoszustw?**

Strategia Cyfryzacji Państwa szeroko ujmuje zagadnienie cyberbezpieczeństwa, jako jednego z filarów cyfrowego rozwoju państwa.

W Strategii przewidziano działania, mające na celu skuteczne zwalczanie cyberprzestępczości, m.in.:

- 1) Wprowadzenie regulacji pozwalających skuteczniej zwalczać cyberprzestępczość, w tym przepisów karnych, przepisów z zakresu zabezpieczenia elektronicznego materiału dowodowego oraz przeciwdziałania kradzieży tożsamości, przepisów dotyczących banków i instytucji finansowych;
- 2) Wzmocnienie wyspecjalizowanych struktur zwalczania cyberprzestępczości w zakresie rozwoju zasobu kadrowego i narzędzi służących do zbierania i analizowania dowodów;
- 3) Podnoszenie potencjału organów ścigania i wymiaru sprawiedliwości;
- 4) Krajowa i międzynarodowa wymiana wiedzy i doświadczeń z zakresu cyberbezpieczeństwa i cyberprzestępczości.

Ponadto, w Strategii zaplanowano działania mające na celu wzmocnienie cyberodporności systemów informacyjnych, a także zwiększenie wśród społeczeństwa wiedzy, kompetencji oraz świadomości cyberzagrożeń.

Niezależnie od powyższego na uwadze mieć należy również ustawę o zwalczaniu nadużyć w komunikacji elektronicznej<sup>2</sup>. Jest ona pierwszą regulacją dotyczącą nadużyć w komunikacji elektronicznej. Ustawa została przyjęta prawie jednogłośnie przez Sejm, co wskazuje na konsensus wśród parlamentarzystów. Było to również dowodem, że regulacja ta jest szczególnie ważna i potrzebna.

Pod pojęciem nadużycia w komunikacji elektronicznej, o którym mowa w ustawie, należy rozumieć świadczenie lub korzystanie z usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi lub osiągnięcie nienależnych korzyści dla podmiotu dopuszczającego się nadużycia w komunikacji elektronicznej, innej osoby fizycznej, osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej.

Ustawa penalizuje zdefiniowane w niej nadużycia w komunikacji elektronicznej, którymi są m.in.: smishing, CLI spoofing i tworzenie sztucznego ruchu.

---

<sup>2</sup> Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej (Dz.U. z 2024 r. poz. 1803 z późn. zm.)

Przepisy ustawy przeciwdziałają oszustwom dokonywanym na szkodę m.in. seniorów. Ograniczają również liczbę fałszywych telefonów, w których oszust podszywał się pod pracownika banku. Blokują fałszywe SMS z linkami do płatności za rzekomo niezapłacony rachunek. Identyfikują i blokują fałszywe strony internetowe banków i instytucji publicznych.

### 1. Zwalczanie fałszywych wiadomości SMS

Zgodnie z ustawą, na podstawie zgłoszeń fałszywych wiadomości SMS, CSIRT NASK tworzy wzorzec fałszywej wiadomości SMS. Istotne znaczenie ma przede wszystkim świadomość społeczeństwa o możliwości zgłoszenia fałszywej wiadomości SMS do CSIRT NASK za pomocą numeru 8080, zdolności analityków w CSIRT NASK do analizy tych wiadomości i tworzenia wzorców oraz współpraca przedsiębiorców telekomunikacyjnych świadczących usługi przesyłania SMS, którzy są podłączeni do systemu telegraf.cert.pl. System ten służy do wymiany informacji o wzorcach złośliwych wiadomości i zarezerwowanych nadpisach. Niezbędna jest ciągła kampania informacyjna o możliwości zgłaszania fałszywych wiadomości SMS do CSIRT NASK.

W 2025 r. CSIRT NASK stworzył 790 wzorców złośliwych wiadomości<sup>3</sup>.

Na ten moment widzimy stały wzrost efektywności blokowania wiadomości. Po wprowadzeniu mechanizmu blokowania wiadomości smishingowych oszuści starają się omijać blokady operatorów zmieniając treść wiadomości, np. poprzez dodawanie nietypowych znaków specjalnych, błędy składniowe oraz celowe literówki, co w rezultacie znacząco obniża ich wiarygodność.

Mechanizm blokowania wiadomości smishingowych należy ocenić pozytywnie, umożliwia on efektywną walkę ze smishingiem.

### 2. Wykaz nadpisów podmiotów publicznych

Ustawa umożliwia podmiotom publicznym zastrzeżenie swojego nadpisu SMS (SMS sender ID) w wykazie nazw i ich skrótów zastrzeżonych dla podmiotów publicznych jako nadpis wiadomości pochodzącej od tego podmiotu publicznego. Wykaz ten jest prowadzony przez CSIRT NASK. Zastrzeżenie nadpisu jest fakultatywne. Podmiot publiczny, który zastrzegł nadpis jest obowiązany do korzystania z usług integratorów usług SMS wpisanych do wykazu integratorów usług SMS dla podmiotów publicznych. W wykazie nadpisów jest obecnie wpisanych ok. 332 nadpisów (stan na 26.05.2026 r.). Wydaje się, że rozwiązanie to wymaga większej promocji wśród podmiotów publicznych, szczególnie wśród jednostek samorządu terytorialnego.

### 3. Zwalczanie fałszywych połączeń głosowych

Numer telefonu nie jest szyfrowany. Oszust może podszyć się pod numer telefonu innej osoby lub instytucji za pomocą internetowych bramek telefonicznych – w tym celu podstawia inny numer, wtedy ofiara widząc na ekranie telefonu znajomy numer może nieświadomie uznać, że dzwoni bliska osoba albo bank, czy inna instytucja. Przestępca wykorzystując zaufanie odbiorcy może ją nakłonić do przekazania danych osobowych, danych o koncie bankowym, haseł i doprowadzić do szkody majątkowej lub osobistej. Takie działania określa się jako CLI spoofing.

Połączenia mające charakter CLI spoofing są blokowane albo usuwana jest prezentacja numeru (CLIR). To ostatnie zachodzi w sytuacji, gdy istnieje duże prawdopodobieństwo, że połączenie ma charakter CLI spoofing, ale dane sygnalizacyjne nie dają pewności.

---

<sup>3</sup> [https://dane.gov.pl/pl/dataset/3828/resource/1035909,statystyki-sms-ow-obsuzonych-przez-cert-polska-oraz-liczba-wytworzonych-wzorcow-faszywych-wiadomosci-sms-122025/table?page=1&per\\_page=20&q=&sort=](https://dane.gov.pl/pl/dataset/3828/resource/1035909,statystyki-sms-ow-obsuzonych-przez-cert-polska-oraz-liczba-wytworzonych-wzorcow-faszywych-wiadomosci-sms-122025/table?page=1&per_page=20&q=&sort=).

Usunięcie prezentacji powoduje, że numer wyświetla się na ekranie telefonu jako numer zastrzeżony, co powinno wywołać wątpliwości u odbiorcy czy nie ma do czynienia z oszustwem.

We wrześniu 2024 r. przedsiębiorcy telekomunikacyjni – operatorzy sieci mobilnej wdrożyli rozwiązania tzw. Bezpiecznej Zatoki, która umożliwia identyfikację, wymianę informacji oraz blokowanie fałszywych połączeń. Szczegóły techniczne dotyczące tego rozwiązania znajdują się w Porozumieniu operatorów sieci mobilnej z Prezesem Urzędu Komunikacji Elektronicznej<sup>4</sup>. Dla mniejszych przedsiębiorców telekomunikacyjnych Prezes Urzędu Komunikacji Elektronicznej wydał rekomendacje określające środki zwalczające fałszywe połączenia głosowe<sup>5</sup>.

Rozwiązanie należy uznać za pozytywne, jednakże jego praktyka wymaga dopracowania – odbierane są pojedyncze sygnały od przedsiębiorców telekomunikacyjnych, że niektóre połączenia były blokowane niezasadnie.

W roku 2025 r. średnia liczba połączeń blokowanych lub z ukrytą prezentacją numeru przekraczała 5 mln tygodniowo, ze znacznym wzrostem w miesiącu przed świętami Bożego Narodzenia. Za pierwsze 4 miesiące 2026 r. odnotowywano podobnie jak w roku poprzednim średnio 5 mln<sup>6</sup> połączeń ukrytych lub zablokowanych tygodniowo. Liczba połączeń blokowanych świadczy o działaniu mechanizmów przeciwdziałających CLI spoofing.

Jednak pomimo wprowadzonych mechanizmów w dalszym ciągu zgłaszane są wnioski konsumentów dot. podejrzenia CLI spoofing. W roku 2025 do UKE wpłynęło 26 takich zgłoszeń od konsumentów, a od stycznia do kwietnia 2026 r. odnotowano 7 takich zgłoszeń. W ramach wydanych rekomendacji Prezesa UKE wskazano również przedsiębiorcom ustalony kanał techniczny, poprzez który mogą zgłaszać przypadki CLI spoofing. Powyższe zgłoszenia poddawane są analizie technicznej w celu ustalenia: potencjalnych błędów w funkcjonowaniu mechanizmów ochronnych oraz korekty ich funkcjonowania.

W 2026 r. rozpoczęły się kontrole w przedsiębiorstwach telekomunikacyjnych w zakresie realizacji obowiązków związanych ze zwalczaniem CLI spoofing. Planowany jest również przegląd rekomendacji Prezesa UKE, którego celem jest optymalizacja środków przeciwdziałających CLI spoofing w oparciu o wnioski wynikające z przekazanych do UKE zgłoszeń oraz obserwacji.

W odniesieniu do przypadków kierowania fałszywych zgłoszeń kierowanych do służb należy zaznaczyć, że dotyczy to zarówno CLI spoofing, jak i połączeń kierowanych na numery alarmowe z wykorzystaniem legalnych urządzeń, w tym urządzeń pozbawionych karty SIM. W latach 2025-2026 wpłynęło jedno pismo z Ministerstwa Spraw Wewnętrznych i Administracji związane z fałszywymi zgłoszeniami, ponadto w przestrzeni publicznej pojawiła się informacja o przypadku zakłócania numeru alarmowego 112 przez osobę dzwoniącą z telefonu bez karty SIM. W obydwu sytuacjach nie było to podszywanie się pod numer telefonu, a zakłócenie funkcjonowania numeru alarmowego poprzez ustawiczne dzwonicie przez użytkownika. Urząd Komunikacji Elektronicznej i Ministerstwo Spraw Wewnętrznych i Administracji podejmą współpracę roboczą w celu ustalenia skali, zakresu i pochodzenia tego typu zdarzeń.

Ustawa dała podstawę do funkcjonowania wykazu numerów służących wyłącznie do odbierania połączeń głosowych. Wykaz ten jest prowadzony przez Prezesa Urzędu Komunikacji Elektronicznej. Wykaz ma służyć ograniczeniu podszywania się pod numery

---

<sup>4</sup> <https://uke.gov.pl/akt/porozumienie-prezesa-uke-i-operatorow-w-sprawie-cli-spoofingu,522.html>

<sup>5</sup> <https://bip.uke.gov.pl/bezpieczenstwo/rekomendacje-prezesa-uke-dotyczace-cli-spoofing,23.html>

<sup>6</sup> Szacunki na podstawie danych otrzymanych od 4 największych operatorów telekomunikacyjnych.

infolinii np. banków czy urzędów – te numery nie służą do dzwonienia do klientów. Zdarzały się jednak przypadki, że oszust wykorzystywał numer infolinii banku i dzwonił do nieświadomej ofiary przedstawiając się jako pracownik banku.

Przedsiębiorca telekomunikacyjny ma obowiązek automatycznie blokować numer wpisany do wykazu. Obecnie w wykazie widnieje 70 numerów. Niezbędna jest akcja promocyjna tego rozwiązania.

#### 4. Lista ostrzeżeń

Przepisy ustawy dały podstawę do funkcjonowania listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzenia mieniem użytkowników internetu. Uprawnienie do blokowania domen znajdujących się na liście mają przedsiębiorcy telekomunikacyjni, którzy przystąpili do porozumienia z Prezesem UKE, Ministrem Cyfryzacji i NASK-PIB. W chwili obecnej 16 przedsiębiorców telekomunikacyjnych dołączyło do porozumienia<sup>7</sup>.

Podmiot dysponujący tytułem prawnym do domeny umieszczonej na liście ma prawo zgłosić sprzeciw wobec umieszczenia na liście do Prezesa Urzędu Komunikacji Elektronicznej, co zapewnia prawo do odwołania się.

Łącznie w 2025 r. wpisano na listę 244 341 fałszywych domen. Rozwiązanie to należy ocenić pozytywnie – skutecznie ogranicza posługiwanie się fałszywymi domenami.

#### 5. Straty pokrzywdzonych

Według danych pozyskanych z Centralnego Biura Zwalczania Cyberprzestępczości w 2025 r. pokrzywdzeni zadeklarowali następujące straty wynikające z przestępstw związanych z nadużyciami w komunikacji elektronicznej:

| Rodzaj strat                                                                                     | Kwota strat w 2025 r.  |
|--------------------------------------------------------------------------------------------------|------------------------|
| straty deklarowane przez pokrzywdzonych przestępstwem sztucznego ruchu                           | 248 770,00 zł          |
| straty deklarowane przez pokrzywdzonych przestępstwem smishingu                                  | 1 158 113,00 zł        |
| straty deklarowane przez pokrzywdzonych przestępstwem CLI spoofing                               | 1 632 616,00 zł        |
| straty deklarowane przez pokrzywdzonych przestępstwem nieuprawnionej zmiany informacji adresowej | 8 579,00 zł            |
| <b>SUMA</b>                                                                                      | <b>3 048 078,00 zł</b> |

W przedmiocie strat spowodowanych przez nadużycia w komunikacji elektronicznej bardzo ciężko jest je oszacować w pełni. Są to dynamicznie rozwijające się zjawiska. Realne straty są niemożliwe do wyliczenia ze względu na to, że często pokrzywdzeni nie zgłaszają przestępstw albo zgłaszają w sposób niekompletny. Ponadto często skutkiem nadużyć w komunikacji elektronicznej jest np. wyciek danych - trudno jest oszacować straty wynikające z takiego zdarzenia.

#### 6. Monitorowanie stosowania przepisów ustawy

Prezes Urzędu Komunikacji Elektronicznej co roku do 31 marca przedstawia sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii oraz Ministrowi Cyfryzacji roczne sprawozdanie z wykonywania swoich obowiązków i uprawnień wynikających z ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej.

<sup>7</sup> [https://dane.gov.pl/pl/dataset/4640,Strony-porozumienia-w-sprawie-listy-ostrzezen/resource/77081,strony-porozumienia-w-sprawie-listy-ostrzezen/table?page=1&per\\_page=50&q=&sort=](https://dane.gov.pl/pl/dataset/4640,Strony-porozumienia-w-sprawie-listy-ostrzezen/resource/77081,strony-porozumienia-w-sprawie-listy-ostrzezen/table?page=1&per_page=50&q=&sort=)

Informacja ministra cyfryzacji na temat wniosków z funkcjonowania ustawy o zwalczaniu nadużyć w komunikacji elektronicznej była przedmiotem obrad sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii w dniu 5 marca 2025 r.<sup>8</sup>

Ministerstwo Cyfryzacji co kwartał monitoruje przestępstwa związane z nadużyciami w komunikacji elektronicznej – wspólnie z Centralnym Biurem Zwalczania Cyberprzestępczości oraz z Prokuraturą Krajową.

**Ad 7) Czy rząd analizował ryzyko całkowitego uzależnienia obywateli od systemów cyfrowych?**

W Strategii Cyfryzacji Państwa ujęto działania wspierające suwerenność technologiczną oraz wzmacniające krajową bazę technologiczno-przemysłową, m.in.:

- Zwiększenie bezpieczeństwa łańcuchów dostaw w wymiarze krajowym i międzynarodowym (zarówno w wymiarze sprzętowym jak i oprogramowania), kierując się interesami bezpieczeństwa narodowego oraz polskiej gospodarki;
- Wprowadzenie mechanizmu umożliwiającego wykluczenie produktów ICT, rodzajów usług ICT lub konkretnych procesów ICT pochodzących od dostawców wysokiego ryzyka;
- Rozwijanie krajowego systemu certyfikacji cyberbezpieczeństwa przez wdrażanie europejskich i tworzenie krajowych programów certyfikacji cyberbezpieczeństwa dla produktów, usług, procesów (ICT) oraz kompetencji personelu;
- Realizacja działań prowadzących do stworzenia polskich rozwiązań cyberbezpieczeństwa, w tym programów i projektów badawczo-rozwojowych i innowacyjnych, zarówno sprzętowych, jak i programowych, co pozwoli na budowę krajowych kompetencji technologicznych i przemysłowych oraz zwiększenie suwerenności technologicznej Polski;
- Realizacja inicjatyw wykorzystujących technologie przełomowe (w tym sztuczną inteligencję) na potrzeby cyberbezpieczeństwa.

Działania te umożliwią wykluczenie dostawców wysokiego ryzyka w przypadku zidentyfikowania zagrożeń dla bezpieczeństwa państwa, tym samym, zapewnienie obywatelom dostępu do bezpiecznych i pewnych produktów, usług i procesów ICT.

**Ad 8) Jakie procedury awaryjne przewidziano na wypadek dużych awarii systemów teleinformatycznych?**

W Strategii Cyfryzacji Państwa zaprojektowano działania, których realizacja wzmocni cyberodporność systemów informacyjnych, co ma kluczowe znaczenie dla państwa, w szczególności w sytuacjach kryzysowych.

W Strategii zaplanowano m.in.:

- 1) wzmacnianie roli Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa oraz Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, co pozwoli zwiększyć efektywność systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni;
- 2) wzmacnianie potencjału instytucji odpowiedzialnych za zapewnianie cyberbezpieczeństwa na poziomie krajowym, ze szczególnym uwzględnieniem zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego;
- 3) wprowadzenie rozwiązania umożliwiającego szybkie pozyskiwanie usług i produktów związanych z cyberbezpieczeństwem w pilnych przypadkach dotyczących bezpieczeństwa państwa, przy jednoczesnym zachowaniu transparentności procesu zakupowego oraz określeniu szczególnego trybu

---

<sup>8</sup> <https://www.sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?sknr=CNT-43>.

zastosowania tego rodzaju procedury, co pozwoli uniknąć długotrwałych postępowań przetargowych negatywnie oddziałujących na cyberbezpieczeństwo państwa;

- 4) monitorowanie bezpieczeństwa systemów i rejestrów państwowych w trybie 24/7 przez zespoły cyberbezpieczeństwa w podmiotach je utrzymujących, stałe podnoszenie zdolności do reagowania na incydenty oraz przez wdrażanie nowych rozwiązań technicznych, proceduralnych i systemowych, jak również przeprowadzanie cyklicznych testów ciągłości działania oraz włączenie aspektów cyberbezpieczeństwa na jak najwcześniejszym etapie rozwoju i utrzymania;
- 5) opracowanie Krajowego planu reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę;
- 6) rozwijanie zdolności w zakresie rozpoznawania zagrożeń w cyberprzestrzeni (ang. Cyber Threat Intelligence) oraz analityki i przewidywania rozwoju sytuacji w cyberprzestrzeni (ang. Cyber Foresight), tak aby móc odpowiadać na aktualne wyzwania. Działania te będą mogły być wykorzystane na potrzeby zarządzania ryzykiem i wprowadzania mechanizmów korygujących cele operacyjne;
- 7) wspieranie procesów przygotowania i wdrażania planów awaryjnych przez przedsiębiorców telekomunikacyjnych, umożliwiających nieprzerwane świadczenie usług w sytuacjach szczególnych zagrożeń oraz realizację zobowiązań związanych z obronnością, bezpieczeństwem i porządkiem publicznym.

Niezależnie od powyższego kwestia zapewnienia ciągłości działania usług, zwłaszcza w sytuacji dużych awarii, jest w Polsce uregulowana przepisami prawa, a znaczący krok w tym zakresie stanowi nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa<sup>9</sup> (UKSC).

Przepisy te rezygnują z dotychczasowego pojęcia operatorów usług kluczowych (OUK) na rzecz znacznie szerszej grupy podmiotów kluczowych oraz podmiotów ważnych.

#### 1. Obowiązki podmiotów kluczowych i ważnych

Wymienione podmioty mają bezwzględny obowiązek wdrożenia rygorystycznego systemu zarządzania bezpieczeństwem informacji. Zgodnie z art. 8 ust. 1 pkt 2 lit. f znowelizowanej UKSC, podmioty kluczowe i ważne odpowiadają za:

- Wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania – umożliwiających ciągłe i niezakłócone świadczenie usług oraz zapewniających poufność, integralność, dostępność i autentyczność informacji.
- Plany awaryjne oraz plany odtworzenia działalności – pozwalające na odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków.

Gwarantuje to, że w sytuacji krytycznej podmioty te dysponują konkretnymi procedurami pozwalającymi na szybkie przywrócenie systemów do działania.

#### 2. Szczególny reżim dla Infrastruktury Krytycznej (IK)

Szczególny reżim prawny obowiązuje w stosunku do infrastruktury krytycznej (IK). Zgodnie z ustawą o zarządzaniu kryzysowym (UZK) oraz Narodowym Programem Ochrony Infrastruktury Krytycznej, właściciele i posiadacze IK muszą obligatoryjnie:

- 1) Przygotowywać szczegółowe plany ochrony.

---

<sup>9</sup> Dz. U. z 2026 r. poz. 20 i 252

- 2) Utrzymywać własne systemy rezerwowe, które podtrzymają funkcjonowanie infrastruktury do czasu jej pełnego odtworzenia.

### 3. Procedury na szczeblu krajowym i rządowym

W przypadku awarii o charakterze ogólnokrajowym zastosowanie znajdują procedury ujęte w Krajowym Planie Zarządzania Kryzysowego (KPZK). Jest to dokument planistyczny przygotowywany przez Rządowe Centrum Bezpieczeństwa (RCB) we współpracy z ministerstwami, urzędami centralnymi i województwami, oparty na przepisach UZK.

KPZK dzieli się na kluczowe sekcje strukturalne:

- Część A: Zawiera charakterystykę zagrożeń oraz ocenę ryzyka wystąpienia zakłóceń w funkcjonowaniu sieci i usług telekomunikacyjnych. Określa również zadania uczestników zarządzania kryzysowego w formie tzw. siatki bezpieczeństwa dla faz zapobiegania i przygotowania.
- Część B: Wyznacza podmioty odpowiedzialne za monitorowanie i reagowanie na duże zakłócenia systemów i sieci teleinformatycznych. Reguluje ponadto procedurę SPO-16, czyli zasady zwoływania i obsługi posiedzenia Zespołu do spraw Incydentów Krytycznych.

### 4. Krajowy plan reagowania na incydenty cyberbezpieczeństwa na dużą skalę

Uzupełnieniem systemu będzie specjalny, będący na etapie finalnych prac, „Krajowy plan reagowania na incydenty i sytuacje kryzysowe w cyberbezpieczeństwie na dużą skalę”. Dokument ten, wydawany na podstawie art. 72a ustawy o UKSC, usystematyzuje i doprecyzuje zadania organów państwa w układzie 4 faz zarządzania kryzysowego: zapobiegania, przygotowania, reagowania, odbudowy. Plan ten jednoznacznie wyszczególni cele działań w cyberprzestrzeni oraz zadania organów odpowiedzialnych za zarządzanie incydentami masowymi.

#### **Ad 9) Czy Ministerstwo posiada dane dotyczące skali problemów obywateli z e-usługami publicznymi?**

Informacje dotyczące skali problemów obywateli z e-usługami publicznymi są zbierane na bieżąco przez Zespoły Wsparcia Centralnego Ośrodka Informatyki pozostające w bezpośrednim kontakcie z obywatelami i instytucjami zgłaszającymi problemy. Przykładowo, w okresie od 1 stycznia do 31 maja 2026 r. zarejestrowano 18 018 zgłoszeń (5420 incydentów oraz 12 598 wniosków o usługę). Zgłoszenia te są analizowane pod kątem ich częstotliwości i tematyki, a na ich podstawie usługi są stale ulepszone.

Dodatkowo, regularnie analizowane są wyniki ankiet uzupełnianych przez obywateli i podmioty zgłaszające problemy – wyniki tych analiz również przyczyniają się do bieżącego usuwania utrudnień oraz stałego ulepszania istniejących e-usług publicznych.

#### **Ad 10) Czy obecny model cyfryzacji państwa nie prowadzi do wykluczenia części obywateli z dostępu do podstawowych usług?**

Ministerstwo Cyfryzacji poprzez swoje działania zmierza do zwiększenia liczby spraw załatwianych za pomocą środków elektronicznych. Działania służące realizacji tego założenia, ujęte zostały w Strategii Cyfryzacji Państwa i opisane są kierunkowo w odpowiedzi na powyższe pytania.

Jednocześnie należy podkreślić, że Ministerstwo Cyfryzacji stoi na stanowisku, że tworzenie nowych e-usług publicznych czy podnoszenie użyteczności już istniejących nie powinno pozbawiać obywateli możliwości załatwienia sprawy w sposób tradycyjny (w urzędzie). Skorzystanie z elektronicznych usług publicznych powinno mieć charakter

dobrowolny i to obywatel powinien mieć możliwość wyboru, czy chce załatwić sprawę cyfrowo czy tradycyjnie.

Odnosząc się wprost do zadanego pytania należy zauważyć, że w istocie obserwuje się zjawisko przeciwne. Postępująca cyfryzacja przyczynia się do zwiększenia dostępności podstawowych usług, które mogą być realizowane w sposób szybszy i bardziej efektywny, bez konieczności osobistego stawiennictwa w miejscu ich świadczenia. Coraz większa liczba spraw może być załatwiona zdalnie, bez wychodzenia z domu.

Informacje o dostępnych usługach i rozwiązaniach cyfrowych są szeroko upowszechniane za pośrednictwem kampanii informacyjnych prowadzonych w mediach, których celem jest zarówno zwiększenie świadomości obywateli, jak i zachęcenie do korzystania z e-usług.

Jednocześnie osoby zagrożone wykluczeniem cyfrowym nie pozostają bez wsparcia. Należy tutaj wspomnieć o projekcie realizowanym ze środków FERS pn. Kluby Rozwoju Cyfrowego (KRC), gdzie planowane jest utworzenie ponad 2000 KRC w chętnych gminach w całej Polsce. W ramach KRC działają wykwalifikowani edukatorzy wspierający mieszkańców w rozwijaniu kompetencji cyfrowych oraz rozwiązywaniu bieżących problemów związanych z korzystaniem z technologii. Wsparcie to obejmuje m.in. szkolenia, warsztaty oraz indywidualne konsultacje, a także działania w zakresie bezpiecznego korzystania z internetu i zasad higieny cyfrowej. Obecnie w ramach pilotażu powstało 40 KRC, natomiast w rozpoczętym etapie Skalowania został zakończony nabór na Operatorów, którzy będą przygotowywali oraz prowadzili pozostałe KRC w Polsce. Więcej informacji o projekcie dostępnych jest na stronie: [kompetencjacyfrowe.gov.pl](https://kompetencjacyfrowe.gov.pl).

Ponadto, wykluczenie cyfrowe może być spowodowane także brakiem dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych i gospodarczych. Zwiększona świadomość w podmiotach publicznych i gospodarczych kwestii związanych z zapewnieniem i wdrażaniem dostępności cyfrowej, większa liczba specjalistów dostępności cyfrowej, a także podejmowane przez Ministra Cyfryzacji działania kontrolne wynikające z ustawy PAD przyczyniają się do poprawy dostępności cyfrowej stron internetowych i aplikacji mobilnych. Poprawa dostępności cyfrowej będzie czynnikiem niwelującym wykluczenie cyfrowe, zwłaszcza osób starszych i z niepełnosprawnościami.

Z wyrazami szacunku

Paweł Olszewski

Sekretarz Stanu

/dokument podpisany elektronicznie/

**Do wiadomości:**

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych