Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.60.2026
Warszawa, 27 kwietnia 2026 r.

Szanowna Pani
Magdalena Biejat
Wicemarszałek Senatu RP

Dot. pisma z 18 marca 2026 r. w sprawie oświadczenia złożonego przez senatora Bogdana Borusewicza podczas 54. Posiedzenia Senatu w dniu 12 marca 2026 r. (BPS/043-54-1420/26)

Szanowna Pani Marszałek,

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". 9 stycznia br. ustawa została zawetowana przez Prezydenta RP.

Celem ustawy było zwiększenie ochrony użytkowników internetu przed nielegalnymi treściami, poprzez umożliwienie wydawania nakazów podjęcia działań przeciwko nielegalnym treściom polegających na uniemożliwieniu dostępu do nielegalnych treści występujących w usłudze świadczonej przez dostawcę usług pośrednich. Jako nielegalne zakwalifikowano m.in. treści wypełniające znamiona z 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.

Polska jest jednym z ostatnich krajów w Unii Europejskiej, które jeszcze nie zaimplementowały do krajowego porządku prawnego przepisów DSA. Weto Prezydenta uniemożliwiło ten proces.

Ministerstwo Cyfryzacji przygotowało nowe projekty wdrażające DSA. Przepisy zostały ujęte w dwóch projektach, aby przyspieszyć wdrożenie. Projekty ustaw zostały wpisane do wykazu prac legislacyjnych i programowych Rady Ministrów pod numerami UC140 i UC141. W dniach 6-20 lutego br. odbył się proces ich uzgodnień i konsultacji. Projekty zostały opublikowane na stronach RCL[1].

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej[2] weszła w życie 25 września 2023 r. Ustawa została przyjęta prawie jednogłośnie przez Sejm, co wskazuje na konsensus wśród parlamentarzystów.

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.

[1] https://legislacja.rcl.gov.pl/projekt/ oraz https://legislacja.rcl.gov.pl/projekt/12406905
[2] Dz.U. z 2024 r. poz. 1803.

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

ul. Królewska 27
00-060 Warszawa

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

Przepisy ustawy przeciwdziałają oszustwom dokonywanym na szkodę m.in. seniorów. Ograniczają 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.

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[3].

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.

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. 339 nadpisów (stan na 31.03.2026 r.). Wydaje się, że rozwiązanie to wymaga większej promocji wśród podmiotów publicznych, szczególnie wśród jednostek samorządu terytorialnego.

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.

[3] 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=.

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. 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 dotyczącego tego rozwiązania znajdują się w Porozumieniu operatorów sieci mobilnej z Prezesem Urzędu Komunikacji Elektronicznej[4]. Dla mniejszych przedsiębiorców telekomunikacyjnych Prezes Urzędu Komunikacji Elektronicznej wydał rekomendacje określające środki zwalczające fałszywe połączenia głosowe[5].

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 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 69 numerów. Niezbędna jest akcja promocyjna tego rozwiązania.

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[6].

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.

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

[4] https://uke.gov.pl/akt/porozumienie-prezesa-uke-i-operatorow-w-sprawie-cli-spoofingu,522.html.
[5] https://bip.uke.gov.pl/bezpieczenstwo/rekomendacje-prezesa-uke-dotyczace-cli-spoofing,23.html.
[6] 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= .

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
SUMA	3 048 078,00 zł

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.

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 o zwalczaniu nadużyć w komunikacji elektronicznej.

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 05 marca 2025 r.[7]

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

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

[7] https://www.sejm.gov.pl/Sejm10.nsf/biuletyn.xsp?skrnr=CNT-43.

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

ul. Królewska 27
00-060 Warszawa