|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Instytucja | Jednostka redakcyjna | Treść uwagi | Odniesienie |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Uwaga ogólna | I. [UWAGA OGÓLNA]  (1.) Izba od wielu lat konsekwentnie popiera wszelkie słuszne inicjatywy mające na celu zwalczanie nadużyć na rynku telekomunikacyjnym (w tym zakresie zostały przedstawione przynajmniej dwukrotnie rozwiązania legislacyjne służące zwalczaniu nadużyć).  (2.) Aby jednak takie działania były efektywne, konsekwentnie wnosimy o precyzyjne uregulowanie obowiązków na tym polu.  Wszelkie obowiązki powinny być określone w sposób maksymalnie precyzyjny i wyczerpujący. | **Uwaga wyjaśniona**  Przepisy projektu ustawy są adekwatne do obecnej sytuacji. |
|  | Unia Metropolii Polskich | Uwaga ogólna | Nieprawidłowo ustalony zakres projektu w stosunku do jego tytułu oraz przeznaczenia.  Jeżeli projekt ma dotyczyć zwalczania nadużyć powinien nakładać obowiązki na podmioty dokonujące takich nadużyć lub zakazywać ich im dokonywania takich czynności.  Obowiązku dotyczące podmiotów publicznych, które mogą stanowić „ochronę” przed nadużyciami powinny być zamieszczone w przepisach stanowiących podstawę dla działalności jst w zakresie informatyzacji lub cyberbezpieczeństwa np. w ustawie o informatyzacji ale najlepiej w ustawie KSC.  Nie należy dążyć do dalszego rozchwiania systemu i tworzenia obowiązków dla podmiotów publicznych w różnych ustawach szczegółowych, które *de facto* dotyczą ochrony bezpieczeństwa informacyjnego. | **Uwaga wyjaśniona**  Projektowany akt prawny znajduje się na styku dziedziny prawa telekomunikacyjnego i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa. Z tego względu, a także ze względu na doniosłość materii regulowanej, zasadne jest aby przepisy te znalazły się w odrębnym akcie prawnym.  Odpowiednie przepisy dotyczące nadużyć telekomunikacyjnych zostaną usunięte (lub przeniesione) z ustawy - Prawo komunikacji elektronicznej na kolejnym etapie prac legislacyjnych (zgodnie z projektem z 5 maja 2022 r. przepisem do usunięcia jest m.in. art. 173 PKE).  Art. 97 ust. 2 Europejskiego Kodeksu Łączności Elektronicznej odnosi się do obowiązku zapewnienia przez państwo członkowskie, aby właściwy (właściwe organ (organy) mógł (mogły) wymagać od przedsiębiorców komunikacji elektronicznej zablokowania incydentalnego dostępu do numerów lub usług, gdy jest to związane z oszustwem lub nadużyciem.  Wdrożenie rzeczonego przepisu EKŁE stanowi projektowany art. 343 PKE, który również zostanie przeniesiony do projektowanej ustawy o zwalczaniu nadużyć w komunikacji elektronicznej, w zakresie w jakim kompetencje Prezesa Urzędu Komunikacji Elektronicznej są wykonywane w „uzasadnione ochroną użytkowników końcowych przed nadużyciami telekomunikacyjnymi”. |
|  | Unia Metropolii Polskich | Uwaga ogólna | Ustawa nakłada pewne zadania na przedsiębiorców telekomunikacyjnych i w przypadku CLI spoofing i jest zrozumiałe. Są też określone obowiązki nakładane na operatorów poczty e-mail. Jednakże projektodawca pozostawia poza zakresem regulacji niezagospodarowany obszar komunikacji elektronicznej w postaci różnego rodzaju komunikatorów.  Jest to tym bardziej dziwne, że w projekcie zastosowano szeroką definicja „usług komunikacji interpersonalnej” a jednocześnie w dalszej części nie ma słowa o komunikatorach i formach świadczących te usługi. Młode pokolenie nie korzysta z SMSów. Tymi kanałami też posługują się coraz częściej różne instytucje.  Należy zadać pytanie, dlaczego ww. regulacja nie dotyczy tego obszaru. | **Uwaga wyjaśniona**  Ustawa posługuje się szerokim pojęciem usług komunikacji interpersonalnej, gdyż zawiera zarówno przepisy odnoszące się do zwalczania nadużyć w telekomunikacji, jak i te dotyczące poczty internetowej (usługi komunikacji elektronicznej). Projektowana ustawa w szczególności zawiera szereg obowiązków i uprawnień po stronie przedsiębiorców telekomunikacyjnych. Z tej perspektywy wskazane przez zgłaszającego uwagę rozwiązania wiązałoby się z koniecznością analizowania treści komunikatów oraz zestawiania ich z innymi informacjami. Ponadto część komunikacji elektronicznej wykorzystuje szyfrowania end-to-end, więc ich wykrywanie jest niemożliwe. |
|  | Polska Izba Informatyki i Telekomunikacji | Uwaga ogólna | Obecnie obowiązujące przepisy prawa, które jako zasadę przyjmują obowiązek zestawiania połączeń a możliwość ich blokowania traktują jako wyjątki dopuszczalne wyłącznie w przypadkach wskazanych w ustawie, wręcz utrudniają przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć telekomunikacyjnych, zmuszając do dokonywania wyborów pomiędzy walką z nadużyciami telekomunikacyjnymi a bezpieczeństwem regulacyjnym. Pomimo ograniczeń regulacyjnych wynikających z obowiązujących przepisów prawa przedsiębiorcy telekomunikacyjni stanowią pierwszą (i najczęściej niestety ostatnią) linię obrony przed przeróżnymi działaniami przestępczymi przyjmującymi postać nadużyć telekomunikacyjnych. Jednym z podstawowych celów przedsiębiorców telekomunikacyjnych w zakresie zwalczania nadużyć jest ochrona klientów. Przedsiębiorcy telekomunikacyjni podejmowali i podejmują szereg proporcjonalnych działań (zarówno technicznych i organizacyjnych) mających na celu przeciwdziałanie nadużyciom oraz zapewnienie w jak największym stopniu bezpieczeństwa usług świadczonych abonentom. Zgromadzone przez przedsiębiorców telekomunikacyjnych doświadczenia pozwalają stwierdzić, że projektowana ustawa wymaga dalszych prac i zmian zgodnych z postulatami wyrażonymi w niniejszym stanowisku, gdyż w obecnym kształcie projektowane przepisy nie do końca prawidłowo rozkładają ciężar odpowiedzialności za walkę z nadużyciami.  Nadużycia z wykorzystaniem sieci i usług telekomunikacyjnych bez wątpienia są zjawiskiem na tyle społecznie szkodliwym, że wymagają kompleksowych i przemyślanych przepisów, które wyposażałyby przede wszystkim organy, instytucje i służby państwa w narzędzia niezbędne do zwalczania tego zjawiska, gdyż to państwo, a nie przedsiębiorcy, jest odpowiedzialne za walkę z przestępczością, a tym w wielu przypadkach są nadużycia z wykorzystaniem sieci i usług telekomunikacyjnych. Jednoczenie takie przepisy powinny umożliwiać przedsiębiorcom telekomunikacyjnym (operatorom i dostawcom usług) podejmowanie działań mających na celu zwalczanie nadużyć, w ramach obsługi ruchu i świadczenia usług telekomunikacyjnych. Przedsiębiorcy telekomunikacyjni mogą wspierać Państwo w walce z tym procederem, w ramach dostępnych możliwości technicznych uwzględniających obecny etap rozwoju sieci i usług telekomunikacyjnych, ale nie mogą Państwa w tym zakresie zastąpić. Natomiast projektowana ustawa składa ciężar ochrony obywateli przed nadużyciami na barki przedsiębiorców telekomunikacyjnych. Nie można również zapominać o tym, że implementacja rozwiązań proponowanych w projektowanej ustawie będzie stanowiła dla przedsiębiorców telekomunikacyjnych kolejne, znaczące koszty oraz wysiłek organizacyjny, kumulujący się z kosztami i nakładem pracy, jaki przedsiębiorcy telekomunikacyjni będą zmuszeni włożyć we wdrożenie wymagań wynikających z projektu ustawy – Prawo komunikacji elektronicznej (oraz ustawy ją wprowadzającej) oraz projektowanej ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa. Nie sposób nie zauważyć, że w chwili obecnej Minister Cyfryzacji prowadzi prace legislacyjne nad projektami trzech ustaw, z których każda będzie miała istotny wpływ na funkcjonowanie rynku telekomunikacyjnego i każda będzie oznaczać dla przedsiębiorców telekomunikacyjnych nowe obowiązki oraz znaczne koszty zarówno dostosowawcze jak i utrzymaniowe.  Operatorzy budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów.  Fakt, że przestępcy wykorzystują sieci i usługi telekomunikacyjne do popełniania przestępstw można porównać do sytuacji popełnienia przestępstwa z użyciem noża – nie jest winą ani odpowiedzialnością producenta i sprzedawcy noża, że przestępca wykorzystał nóż do złamania prawa. Procesy zwalczania nadużyć muszą być kształtowane przede wszystkim z myślą o efektywnym ściganiu i karaniu przestępców przez powołane do tego służby i organy Państwa, jednocześnie dając przedsiębiorcom telekomunikacyjnym możliwość podejmowania działań anty-fraudowych, mieszczących się w zakresie posiadanych przez przedsiębiorców możliwości technicznych i organizacyjnych.  Wysiłki przedsiębiorców telekomunikacyjnych na rzecz ograniczenia zjawiska nadużyć w komunikacji elektronicznej nie przyniosą oczekiwanych rezultatów tak długo, jak długo sprawcy tych naruszeń będą pozostawali nieustaleni i bezkarni. Proceder nadużyć kwitnie, gdyż jest postrzegany przez przestępców jako bezpieczne źródło nielegalnego zarobku, gdyż możliwość zagarnięcia znacznych pieniędzy idzie w parze ze znikomym ryzykiem wykrycia i ukarania.  Podsumowując tę część pragniemy podkreślić, że:  1. zwalczanie nadużyć telekomunikacyjnych, przynajmniej tych, które są przestępstwami w rozumienia prawa karnego, jest i powinno być obowiązkiem i odpowiedzialnością powołanych do ścigania przestępstw służb i organów Państwa;  2. sprawcy, którzy dopuszczają się nadużyć, powinni być wykrywani przez powołane do tego służby i organy, a następnie stawiani przed wymiarem sprawiedliwości;  3. przedsiębiorcy telekomunikacyjni powinni mieć prawo do podejmowania proporcjonalnych działań mających na celu identyfikowanie, zapobieganie i zwalczanie nadużyć telekomunikacyjnych, wspierając w ten sposób wysiłki służb i organów Państwa na rzecz ograniczenia zjawiska nadużyć w komunikacji elektronicznej. | **Uwaga wyjaśniona**  W projekcie zostały wprowadzone przepisy karne.  Poprzez nałożenie obowiązków z zakresu przeciwdziałania i zwalczania nadużyć w komunikacji elektronicznej przedsiębiorcy telekomunikacyjni uzyskają również niezbędne kompetencje do podejmowania działań w tym zakresie. |
|  | Polska Izba Informatyki i Telekomunikacji | Uwaga ogólna | II. Prawa, obowiązki i kary  Zasadą na gruncie projektowanej ustawy powinno być uprawnienie dla przedsiębiorców telekomunikacyjnych do zwalczania nadużyć w komunikacji elektronicznej. Wyjątki od tej zasady powinny dotyczyć tylko tych przypadków, w których można precyzyjnie określić zakres czynności, jakie mają być powinnością przedsiębiorcy telekomunikacyjnego – w tych przypadkach w grę może wchodzić obowiązek, ale bez konieczności obwarowywania jego wykonania ryzykiem kary pieniężnej.  Każdy większy przedsiębiorca telekomunikacyjny posiada w swoich strukturach komórki anty-fraudowe, zatrudnia ekspertów od zwalczania nadużyć, utrzymuje i rozwija procedury i narzędzia IT wspierające ekspertów w detekcji i zwalczaniu nadużyć telekomunikacyjnych. Utrzymywanie i rozwijanie zasobów kadrowych i technicznych to wymierny koszt, który każdy operator traktuje jako koszt konieczny, bez którego straty ponoszone przez przedsiębiorców telekomunikacyjnych i abonentów byłby jeszcze większe. Straty ponoszone przez przedsiębiorców telekomunikacyjnych mają charakter zarówno wizerunkowy jak i majątkowy, gdyż wiele ze scenariuszy nadużyciowych jest wprost wymierzonych w przedsiębiorców telekomunikacyjnych albo szkodzi przedsiębiorcom telekomunikacyjnym niejako w ramach efektów ubocznych działań przestępców. Zresztą jest to odzwierciedlone w samej definicji „nadużycia w komunikacji elektronicznej”, gdzie jedną z przesłanek jest szkoda przedsiębiorcy telekomunikacyjnego. Na poziomie hurtowego rynku telekomunikacyjnego operatorzy rozliczają się wzajemnie za terminowany ruch, co oznacza, że operator abonenta inicjującego połączenie albo wysyłającego wiadomość SMS płaci określoną stawkę hurtową operatorowi abonenta odbierającego połączenie albo SMS. Dodatkowy poziom hurtowych rozliczeń międzyoperatorskich pojawia się przy połączeniach międzynarodowych i realizowanych w roamingu międzynarodowym. Konieczność płacenia za zakańczanie połączeń w relacjach hurtowych oznacza, że nadużycia telekomunikacyjne, generujące istotne ilości ruchu, dla operatorów oznaczają niechciane i nieuzasadnione koszty, które są liczone w setkach tysięcy złotych miesięcznie. Jednocześnie na poziomie detalicznym operatorzy muszą i chcą walczyć z nadużyciami telekomunikacyjnymi w trosce o bezpieczeństwo swoich klientów, gdyż niezwykle konkurencyjny, polski rynek telekomunikacyjny nie pozostawia miejsca do działania dla dostawców usług, którzy nie są gotowi zapewnić swoim abonentom najwyższych możliwych standardów bezpieczeństwa. Wszystko to powoduje, że zwalczanie nadużyć w komunikacji elektronicznej jest w interesie zarówno przedsiębiorców telekomunikacyjnych jak i abonentów korzystających z tych usług. Z tego też względu przedsiębiorcy telekomunikacyjni nie potrzebują dodatkowej motywacji do walki z nadużyciami, w szczególności w postaci obowiązków pod groźbą kary, potrzebują natomiast wsparcia ze strony organów Państwa i regulatora rynku, w szczególności w postaci przepisów prawa, które zamiast krępować ręce dadzą przedsiębiorcom telekomunikacyjnym uprawienia (nie obowiązki) niezbędne do skutecznej walki z nadużyciami.  Podsumowując wątek dotyczący uprawnień, obowiązków i kar:  1. sprawcy nadużyć w komunikacji elektronicznej powinni ponosić odpowiedzialność za swoje nielegalne działania, w związku z czym konieczne jest utrzymanie w projekcie ustawy przepisów, które przewidują odpowiedzialność karną za naruszenie zakazu nadużyć (art. 16 projektu ustawy) oraz dają Prezesowi UKE możliwość nałożenia kary pieniężnej na sprawcę naruszenia (art. 15 ust. 1 projektu ustawy);  2. projektowana ustawa jako zasadę powinna przewidywać uprawnienie dla przedsiębiorców telekomunikacyjnych do zwalczania nadużyć telekomunikacyjnych;  3. reżim obowiązku dla przedsiębiorców telekomunikacyjnych można sobie wyobrazić jako wyjątek od zasady (jaką powinno być uprawienie) tylko dla tych przypadków, w których da się precyzyjnie opisać zakres czynności, które w interesie publicznym powinni wykonać przedsiębiorcy telekomunikacyjni; przykładowo obowiązek może dotyczyć:  a. blokowania SMS wpisujących się we wzorzec przekazany przez NASK (art. 4 ust. 6 projektu ustawy);  b. blokowania połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych, prowadzonego przez Prezesa UKE (art. 9 ust. 12 projektu ustawy);  4. nie jest konieczne wprowadzanie ryzyka kar pieniężnych za naruszenie obowiązków, które mają ciążyć na przedsiębiorcach telekomunikacyjnych;  5. jeśli jednak w ocenie Projektodawcy takie kary są niezbędne, to powinny one dotyczyć tylko obowiązków wymienionych w punkcie 3 powyżej i powinny mieć charakter fakultatywny (tak jak obecnie w art. 15 ust. 2 projektu ustawy);  6. jeśli Projektodawca chce objąć obowiązkiem i ryzykiem kar obszary inne niż wymienione w punkcie 3 powyżej (np. CLI spoofing – art. 8 w zw. z art. 15 ust. 2 pkt 2) projektu ustawy), to dla każdego takiego obszaru konieczne jest wyznaczenie organu państwa, który będzie identyfikował konkretny ruch będący nadużyciem i przekazywał taką informację przedsiębiorcom telekomunikacyjnym celem zablokowania tego konkretnego ruchu (analogicznie do zaprojektowanego mechanizmu identyfikowania smishingowych wiadomości SMS przez NASK); tak zidentyfikowany przez organ państwa ruch przedsiębiorcy telekomunikacyjni mogą blokować w reżimie obowiązku;  Realizacja powyższych postulatów będzie wymagała przeredagowania szeregu przepisów projektowanej ustawy, które obecnie mówią o obowiązku przedsiębiorcy telekomunikacyjnego, tak, aby obowiązek zastąpić uprawnieniem (możliwością). W szczególności:  • art. 3 ust. 2 projektu ustawy powinien uzyskać następujące brzmienie:  Przedsiębiorca telekomunikacyjny może podejmować proporcjonalne działania mające na celu zapobieganie nadużyciom komunikacji elektronicznej i ich zwalczanie.  • art. 8 projektu ustawy powinien uzyskać następujące brzmienie:  W przypadku uzasadnionego podejrzenia wystąpienia CLI spoofingu przedsiębiorca telekomunikacyjny może zablokować takie połączenie albo wyeliminować prezentację identyfikacji numeru wywołującego. | **Uwaga nieuwzględniona**  Aby skutecznie walczyć z nadużyciami w komunikacji elektronicznej powinien zostać nałożony obowiązek prawny (obowiązki) na przedsiębiorców telekomunikacyjnych. W przypadku przyznania uprawnienia przedsiębiorca telekomunikacyjny mógłby, ale nie musiałby podejmować działań mających na celu zwalczanie nadużyć. |
|  | Polska Izba Informatyki i Telekomunikacji | Uwaga ogólna | **Relacja projektowanej ustawy do przepisów o nadużyciach telekomunikacyjnych w projekcie ustawy – Prawo komunikacji elektronicznej**  Nie sposób nie zauważyć, że zarówno konstrukcja jak i brzmienie niektórych przepisów projektowanej ustawy jest wzorowana albo jest powtórzeniem przepisów o nadużyciach telekomunikacyjnych, obecnych w projektowanej ustawie – Prawo komunikacji elektronicznej. Zakładamy, że Projektodawca przedkładając projektowaną ustawę *o zwalczaniu nadużyć w komunikacji elektronicznej* chciał, aby problematyka ta miała dedykowaną ustawę, w związku z czym konieczne jest usunięcie przepisów dotyczących nadużyć telekomunikacyjnych z projektu ustawy – Prawo komunikacji elektronicznej, tak, aby uniknąć konfliktu pomiędzy przepisami obu tych ustaw.  Z projektu ustawy – Prawo komunikacji elektronicznej usunąć należy następujące przepisy:   * art. 2 pkt 26) projektu PKE (definicja nadużyć telekomunikacyjnych); * art. 173 projektu PKE (określający prawa i obowiązki w zakresie zwalczania nadużyć telekomunikacyjnych); * art. 343 ust. 1 projektu PKE (w zakresie, w jakim przepis ten dotyczy wydawania przez Prezesa UKE decyzji dotyczących nadużyć telekomunikacyjnych); * art. 441 ust. 2 pkt 4) i 5) projektu PKE (przepisy przewidujące możliwość nałożenia kary w kontekście nadużyć telekomunikacyjnych).   Jednocześnie dalszych analiz wymaga to, czy z uwagi na relację obu ustaw usunięcia albo zmian wymagają następujące przepisy projektu ustawy – Prawo komunikacji elektronicznej:   * art. 171 ust. 1 pkt 9) projektu PKE (przepis stanowiący, że jednym z elementów umowy o dostępie w zakresie połączenia sieci ma być opis działań podejmowanych w związku z przypadkami nadużycia telekomunikacyjnego); * art. 211 ust. 4 projektu PKE (odnoszący się do nadużyć telekomunikacyjnych w kontekście decyzji SMP). | **Uwaga częściowo uwzględniona**  w zakresie projektowanych przepisów ustawy - Prawo komunikacji elektronicznej: - art. 173 zostanie usunięty;  - art. 343 w zakresie w jakim dotyczy kompetencji Prezesa Urzędu Komunikacji Elektronicznej związanych z ochroną użytkowników końcowych przed nadużyciami telekomunikacyjnymi (a nie innymi nadużyciami związanymi z wykorzystaniem sieci), zostanie przeniesiony do projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej;  - w zakresie art. 171 i art. 211, użyte tam określenie nadużyć telekomunikacyjnych należy odczytywać uwzględniając przepisy ustawy o nadużyciach w komunikacji elektronicznej.  Projekt ustawy - Prawo komunikacji elektronicznej jest właściwym miejscem jako ustawa holistycznie odnosząca się do zagadnień umowy o połączeniu sieci oraz obowiązków regulacyjnych sensu stricto. |
|  | Polska Izba Komunikacji Elektronicznej | Uwaga ogólna | **Uwagi ogólne**  Szczegółowa analiza projektu ustawy, nie tylko pod względem legislacyjnym, ale również pod względem skuteczności proponowanych rozwiązań w zapobieganiu i zwalczaniu nadużyciom w komunikacji elektronicznej, doprowadziła zrzeszonych w Izbie przedsiębiorców do szeregu wątpliwości. Zdaniem Izby **ustawa w obecnym kształcie nie sprosta rynkowym oczekiwaniom, przede wszystkim ze względu na fakt niedostosowania regulacji do obecnie używanych i ciągle rozwijających się technologii i zabezpieczeń.** Wydaje się, że proponowane rozwiązania nie podążają za realiami rynku, a tym samym nie będą wystarczające do tego, aby wypełnić swoje funkcje. Regulacja nie uwzględnia szeregu nowych i często stosowanych obecnie rozwiązań, przez co pozostaje **niepełna i nieprecyzyjna**. Słowem przykładu można wskazać na kwestie nieuwzględnienia w przepisach dot. CLI spoofing zjawisk związanych z podmianą numeru abonenta (m.in. fraudów na rozliczeniach międzyoperatorskich).  W dalszej mierze należy wskazać, że wątpliwości Izby potęgują **liczne błędy legislacyjne w przepisach projektu**. W szczególności należałoby podkreślić wśród nich szereg przepisów o niskiej precyzji, które dla swojej skuteczności wymagają dopracowania (np. art. 3 ust. 1 pkt 3 i zawarte w nim pojęcie CLI spoofing, błędne pojęcie „nieświadomego rozporządzenia majątkiem”, czy zawężające zastosowanie „podszywania się” pod inny podmiot). Ponadto w niektórych przepisach pojawiają się sprzeczności przyjętej siatki pojęciowej (np. zamienne korzystanie z pojęcia „nadawcy” i „osoby inicjującej”).  Jak wspomniano powyżej, ustawa tego rodzaju – wprowadzająca przepisy związane z wysoce technicznymi kwestiami i pojęciami, a także przepisy przewidujące odpowiedzialność karną i administracyjną, powinna być **całkowicie dopracowana** również pod względem legislacyjnym i redakcyjnym. Stąd też, Izba postuluje, aby projekt ustawy został ponownie szczegółowo przepracowany, a następnie uzupełniony i doprecyzowany. Ustawa w obecnym brzmieniu z dużym prawdopodobieństwem nie będzie właściwie stosowana. Wywoła natomiast szereg nieporozumień i sporów. | **Uwaga wyjaśniona** Momentem na ewentualne doprecyzowanie, czy uzupełnienie regulacji jest właśnie rządowy proces legislacyjny, w tym m.in. przeprowadzone konsultacje publiczne, w których Izba wzięła udział. Szczegółowe odniesienie są zawarte przy konkretnych uwagach. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Uwaga ogólna | Uwaga ogólna  W USTAWIE z dnia 7 października 1999 r. o języku polskim (Dz. U. z 2021 r. poz. 672) w **Art. 4. Język polski jest językiem urzędowym: 1) konstytucyjnych organów państwa;** oraz w **Art. 5. 1. Podmioty wykonujące zadania publiczne na terytorium Rzeczypospolitej Polskiej dokonują wszelkich czynności urzędowych oraz składają oświadczenia woli w języku polskim, chyba że przepisy szczególne stanowią inaczej.** Oznacza to, że również teksty uchwalanych ustaw powinny być w języku polskim, z zastrzeżeniem **Art. 11. Przepisy art. 5–10 nie dotyczą: 5) zwyczajowo stosowanej terminologii naukowej i technicznej;**  Powyższe zastrzeżenie może być skuteczne jedynie, gdy konieczne do wskazania w treści terminy nie mają odpowiedników w języku polskim.  W przypadku treści projektu ustawy (RD402) proponujemy na terminy:   * SMS – krótka wiadomość tekstowa, która w języku polskim, zamiast skrótu SMS, może być opisana terminem **esemes** wraz z możliwością jego odmiany (taki termin występuje w słowniku PWN), * smishing – szalbierczy esemes * CLI spoofing – szalbierczy numer dzwoniącego   Proponując wprowadzenie terminu **szalbierczy** jednoznacznie wskazujemy na negatywny odbiór takiego esemesa oraz rozmowy z podszywającego się numeru dzwoniącego. Termin ten można też używać przypadku phishingu – szalbierczej strony oraz szalbierczego mejla. Tekst tej ustawy może przy tej okazji również wprowadzić polską jednoznacznie zrozumiałą terminologię ostrzegania przed nadużyciami w komunikacji elektronicznej. | **Uwaga nieuwzględniona**  Określenie „szalbierczy” potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, że jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach.  Z tego powodu proponuje się pozostawienie pojęcia „smishing”, które jest powszechnie znane i wykorzystywane.  Słownik języka polskiego PWN dopuszcza także skrótowiec SMS[[1]](#footnote-2). |
|  | R.M. osoba fizyczna | Uwaga ogólna | W ramach ogłoszonego projektu ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402), w ramach konsultacji publicznych, chciałbym zgłosić swoje stanowisko jako osoba fizyczna. Projekt nie przewiduje niezbędnego dla zapewnienia bezpieczeństwa obywateli wprowadzenia rejestru "Do not call". Rejestr ten pozwoliłby na dodanie przez obywateli swojego numeru telefonu do ogólnopolskiej bazy (prowadzonej według mnie przez UKE), a realizujący połączenia telefoniczne z usługami niezamawianymi (co mogłoby też obejmować instytucje chcące wyłudzić dane) musieliby pod groźbą kary weryfikować czy mogą wykonać połączenie z tym numerem. Wśród zapisów Prawa Telekomunikacyjnego (Dz.U.2019.2460 t.j.) znajduje się zapis zabraniający używania urządzeń końcowych i automatycznych systemów wywołujących do celu marketingu bezpośredniego (Art. 172). Niestety, zapis ten nie jest wciąż respektowany przez wiele firm, które realizują szeroko zakrojone kampanie telefoniczne, także z wykorzystaniem automatycznych systemów wywołujących. Często dzieje się to bez udziału człowieka, czasem zaś w sposób mieszany: przełączenie do sprzedawcy następuje po odsłuchaniu automatycznego komunikatu i wciśnięciu konkretnej cyfry na telefonie. Firmy te nieraz odmawiają podania danych rejestrowych, podają fałszywe dane lub w sposób ordynarny kończą rozmowę, jeśli nie przebiega ona po ich myśli (np. odbiorca rozmowy dopytuje się o źródło posiadania numeru telefonu). W Stanach Zjednoczonych oraz innych krajach (np. Australia, Nowa Zelandia, Wielka Brytania) stworzono rejestry nazywane ogólnie "Do not call register" (np. dla USA: https://www.donotcall.gov/). Użytkownik końcowy (osoba fizyczna) może zgłosić fakt, że nie życzy sobie telefonów, zaś firmy muszą się pod groźbą dużych kar do tego życzenia dostosować. W Polsce można by użyć do tego ePUAP. Proponuję rozszerzenie w/w projektu ustawy o taką usługę także zmniejszającą ryzyko phishingu. | **Uwaga wyjaśniona**  Zgodnie z obecnie obowiązującymi przepisami Prawa telekomunikacyjnego przedsiębiorcy mają zakaz używania telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących dla celów marketingu bezpośredniego bez zgody abonenta lub użytkownika końcowego.  Za naruszenie tego zakazu, zgodnie z ogólną zasadą, grozi administracyjna kara pieniężna w wysokości do 3% przychodu ukaranego podmiotu, osiągniętego w poprzednim roku kalendarzowym. Ustawa wprowadziła więc generalny zakaz prowadzenia takiej formy marketingu, chyba że zostanie wyrażona zgoda. Rejestr Do Not Call działałby na odwrotnej zasadzie – abonent musiałby wyraźnie stwierdzić, że nie chce otrzymywać takich informacji i wpisać się do rejestru. |
|  | Polskie Towarzystwo Informatyczne | **Art. 1 pkt 2)** | **ad Art. 1 pkt 2)** zasady wnoszenia sprzeciwu przez nadawcę krótkiej wiadomości tekstowej (SMS), wobec uznania treści takiej wiadomości za wyczerpującą znamiona nadużycia w komunikacji elektronicznej;  Propozycja PTI  Przyjąć, w całym tekście ustawy, dopuszczony przez słownik PWN termin **esemes** (wraz z jego odmianą rzeczownikową) zamiast angielskiego skrótu SMS (patrz „Uwaga ogólna”). | **Uwaga nieuwzględniona**  Słownik języka polskiego PWN dopuszcza także skrótowiec SMS[[2]](#footnote-3). |
|  | Porozumienie Zielonogórskie | Uwaga ogólna | Ustawa powinna w miarę możliwości obejmować również zwalczanie działań wykonywanych spoza kraju. | **Uwaga wyjaśniona**  Ustawa zakłada zwalczanie nadużyć w komunikacji elektronicznej niezależnie od kraju nadawcy. |
|  | Polska Wytwórnia Papierów Wartościowych | Uwaga ogólna | **Uwaga ogólna do projektu ustawy**  W projekcie ustawy zostały użyte określenia i skróty nieznane powszechnie oraz nieostre, takie jak: „standard SMTP (Simple Mail Transfer Protocol)”, „POP3 (Post Office Protocol)”, „IMAP4 (Internet Message Access Protocol)”, „SPF (Sender Policy Framework)”, „DMARC (Domain-based Message Authentication Reporting and Conformance)”, „DKIM (DomainKeys Identified Mail)”. W związku z powyższym proponujemy rozważenie umieszczenie ww. skrótów (wraz z ich rozwinięciem i objaśnieniem) w art. 2 projektu ustawy. | **Uwaga wyjaśniona**  Określenia te zostały wyjaśnione w uzasadnieniu projektu ustawy. |
|  | ZTKIG | Uwaga ogólna | **Uwagi ogólne do projektu**  Każde działanie dotyczące obronności, bezpieczeństwa państwa, bezpieczeństwa i porządku publicznego należy oceniać jako pozytywne.  Bezpieczeństwo jest największą wartością człowieka tuż po zapewnieniu potrzeb biologicznych (fizjologicznych) takich jak sen, pożywienie, picie, warunki bytowe, itp. Dlatego przepisy określające prawa i obowiązki związane z bezpieczeństwem powinny stanowić jednoznaczne normy nie pozwalające na ich dowolną interpretację oraz powinny być łatwe do lokalizacji.  Aktualnie obowiązuje kilkanaście ustaw określających obowiązki i prawa przedsiębiorców telekomunikacyjnych z zakresu bezpieczeństwa i obronności.  Podstawowym aktem prawnym regulującym działalność telekomunikacyjną, jest ustawa z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (tekst jedn. Dz. U. z 2021 r. poz. 576 z późn. zm.), zwana dalej prawem telekomunikacyjnym, i tam powinny być określane wszelkie prawa i obowiązki podmiotów wykonujących działalność telekomunikacyjną.  W myśl § 2 załącznika do rozporządzenie Prezesa Rady Ministrów z dnia 20 czerwca 2002 r. w sprawie „Zasad techniki prawodawczej” (Dz. U. z 2016 r. poz. 283), zwanego dalej rozporządzeniem w sprawie techniki prawodawczej, ustawa powinna wyczerpująco regulować daną dziedzinę spraw, nie pozostawiając poza zakresem swego unormowania istotnych fragmentów tej dziedziny.  Niestety niektóre zakresy regulacji objęte projektem ustawy o zwalczaniu nadużyć w komunikacji elektronicznej są zbieżne z obszarami już regulowanymi w obowiązujących ustawach, co potwierdzają poniżej przytoczone przykłady:  a/ art. 178 ust. 1 pkt 2 prawa telekomunikacyjnego uprawnia Prezesa Urzędu Komunikacji Elektronicznej, zwanego dalej Prezesem UKE, do nakładania w drodze decyzji administracyjnej na przedsiębiorcę telekomunikacyjnego obowiązku ograniczenia niektórych, publicznie dostępnych usług telekomunikacyjnych.  b/ art. 175 c prawa telekomunikacyjnego zobowiązuje przedsiębiorcę telekomunikacyjnego do podejmowania proporcjonalnych i uzasadnionych środków mających na celu zapewnienie bezpieczeństwa i integralności sieci, usług oraz przekazu komunikatów związanych ze świadczonymi usługami, w tym:  1) eliminację przekazu komunikatu, który zagraża bezpieczeństwu sieci lub usług;  2) przerwanie lub ograniczenie świadczenia usługi telekomunikacyjnej na zakończeniu sieci, z którego następuje wysyłanie komunikatów zagrażających bezpieczeństwu sieci lub usług.  Ponadto, ustawy określające prawa i obowiązki uprawnionych podmiotów, o których mowa w art. 179 ust. 3 pkt 1 lit. a prawa telekomunikacyjnego określają uprawnienia tych podmiotów do zarządzenia zastosowania urządzeń uniemożliwiających telekomunikację na określonym obszarze, przez czas niezbędny do wyeliminowania zagrożenia lub jego skutków, z uwzględnieniem konieczności minimalizacji skutków braku możliwości korzystania z usług telekomunikacyjnych. [np. art. 18 c ust. 1 ustawy z dnia 6 kwietnia 1990 r. o Policji (tekst jedn. Dz. U. z 2021 r. poz. 1882 z późn. zm.), zwanej dalej ustawą o Policji].  Mając powyższe przepisy na względzie wydaje się zatem uzasadnione oczekiwanie rozszerzenia regulacji już istniejącej i obowiązującej zamiast projektowania i wydawania kolejnej ustawy regulującej kolejne obowiązki z zakresu bezpieczeństwa i obronności nakładane na przedsiębiorcę telekomunikacyjnego.  Projekt omawianej ustawy powstał i jest procedowany w czasie, gdy na bardzo zawansowanym etapie są prace legislacyjne nad projektem ustawy Prawo komunikacji elektronicznej i nad przepisami wprowadzającymi prawo komunikacji elektronicznej oraz procedowany jest projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, w których określono obowiązki przedsiębiorców telekomunikacyjnych zbieżne z zakresem objętym projektem.  Zasadnym zatem będzie uwzględnienie przedmiotu regulacji objętego projektem w projektowanym Prawie Komunikacji Elektronicznej, gdyż pozytywnym skutkiem takiego działania będzie to, że przepisy będą bardziej czytelne oraz nie będzie dochodziło do różnych definicji lub powieleń definicji tych samych określeń.  Z kolei prawa i obowiązki dostawcy poczty elektronicznej w zakresie objętym projektem, można określić w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (tekst jedn. Dz. U. z 2020 r. poz. 344), zwanej dalej ustawą o świadczeniu usług drogą elektroniczną, która to ustawa przecież reguluje także instytucję poczty elektronicznej.  Jak pokazuje powyższa analiza różne ustawy nakładają na przedsiębiorcę telekomunikacyjnego obowiązek podjęcie określonych działań organizacyjnych i technicznych związanych z realizacją zadań na rzecz obronności i bezpieczeństwa, co wiąże się z ponoszeniem kosztów.  Część tych zadań ma na celu zabezpieczenie infrastruktury, usług, danych lub przekazów telekomunikacyjnych znajdujących się we władaniu przedsiębiorcy telekomunikacyjnego- te zadania są i powinny być realizowane na koszt przedsiębiorcy telekomunikacyjnego.  Są jednak i inne zadania z tego zakresu realizowane na rzecz organów administracji publicznej odpowiedzialnych za obronność i bezpieczeństwo, przykładowo tylko wskazując do takich zadań należą:  - zapewnienie podmiotom właściwym w sprawach bezpieczeństwa warunków technicznych i organizacyjnych dostępu do przekazów i danych telekomunikacyjnych oraz ich utrwalanie (art. 179 ust 3 prawa telekomunikacyjnego),  - zatrzymywanie, przechowywanie, zabezpieczenie niektórych danych telekomunikacyjnych oraz ich udostępniania podmiotom właściwym w sprawach bezpieczeństwa, (art. 180 a prawa telekomunikacyjnego, art. 180 c prawa telekomunikacyjnego, art. 180 d prawa telekomunikacyjnego).  Również obowiązki określone w projekcie realizowane będą na rzecz bezpieczeństwa państwa oraz bezpieczeństwa wewnętrznego i porządku publicznego.  Obowiązki te powinny być w dalszym ciągu realizowanie przez przedsiębiorców telekomunikacyjnych jako zadanie niezwykle istotne dla obronności i bezpieczeństwa, natomiast finansowanie ich winno następować z budżetu państwa.  Rekomendujemy zatem podjęcie działań legislacyjnych dotyczących finasowania niektórych obowiązków realizowanych przez przedsiębiorców telekomunikacyjnych ze środków budżetu państwa. | **Uwaga wyjaśniona w zakresie zasadności objęcia zagadnień nadużyć w komunikacji elektronicznej w odrębnym akcie prawnym**  Ze względu na doniosłość materii nadużyć w komunikacji elektronicznej zasadne jest uregulowanie tych zagadnień w odrębnej ustawie. Znaczna część projektowanych przepisów nie ma swojego odpowiednika w projektowanej ustawie Prawo komunikacji elektronicznej, która jest na zaawansowanym etapie rządowego procesu legislacyjnego.  **Uwaga nieuwzględniona w zakresie postulatu finansowania niektórych obowiązków realizowanych przez przedsiębiorców telekomunikacyjnych ze środków budżetu państwa**  Opisywany ogólnie obowiązek jest częścią prowadzenia działalności telekomunikacyjnej, która jest działalnością regulowaną. |
|  | ZTKIG | Tytuł ustawy | **Tytuł ustawy o zwalczaniu nadużyć w komunikacji elektronicznej**  Wskazane by było wprowadzenie zmiany tytułu ustawy na: „ *ustawa z dnia ……. o zwalczaniu nadużyć w telekomunikacji*” lub też pozostawić tytuł w zaproponowanym brzmieniu przy jednoczesnym zdefiniowaniu w słowniczku projektu definicji legalnej pojęcia „*komunikacji elektronicznej*”.  Dotychczas bowiem nie zdefiniowano pojęcia „*komunikacja elektroniczna*”, gdy tymczasem pojęcie to pojawiło się i jest zdefiniowane w projekcie ustawy Prawo komunikacji elektronicznej. | **Uwaga nieuwzględniona**  Zasadność wprowadzenia legalnej definicji komunikacji elektronicznej powinna zostać ewentualnie rozważana na gruncie projektowanej ustawy - Prawo komunikacji elektronicznej. |
|  | ZTKIG | Art. 1 ust. 1 pkt 3 | **Art. 1 ust. 1 pkt 3**  Proponujemy obowiązki dostawcy poczty elektronicznej określić w ustawie o świadczeniu usług drogą elektroniczną, gdyż jest to właściwe miejsce do zawarcia tego rodzaju regulacji, czego nie można powiedzieć o opiniowanym projekcie. | **Uwaga wyjaśniona**  Obowiązki dostawcy poczty elektronicznej mają na celu przeciwdziałanie spoofowaniu poczty elektronicznej, dlatego zasadne jest umieszczenie tych przepisów w projekcie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. |
|  | Porozumienie Zielonogórskie | Art. 2 pkt 2 | W art. 2. Rozszerzyć definicję dostawcy poczty elektronicznej o spółki cywilne oraz m.in. jawne. Te spółki nie mają osobowości prawnej ani nie są osobami fizycznymi więc nie spełniają kryteriów z definicji | **Uwaga wyjaśniona**  Definicja dostawcy poczty elektronicznej obejmuje jednostki organizacyjne nieposiadające osobowości prawnej, a więc również wszystkie spółki osobowe wskazane w Kodeksie spółek handlowych.  Ponadto spółka cywilna jest jednostką organizacyjną, także definicja również obejmuje tę spółkę. |
|  | ZTKIG | Art. 2 pkt 3 | **Art. 2 ust. 1 pkt 3**  Definicję legalną pojęcia „komunikatu elektronicznego” należałoby zaczerpnąć z projektu ustawy Prawo komunikacji elektronicznej (Projekt z dnia 5 maja 2022 r.).  Definicję komunikatu elektronicznego w projekcie w porównaniu do definicji zawartej w art. 1 pkt 19 projektu PKE rozszerzono o frazę: *„… lub usług komunikacji interpersonalnej niewykorzystujących numerów*;”  **Jest to argument przemawiający za tym, aby regulacje objęte projektem umieścić w prawie telekomunikacyjnym lub w projektowanej ustawie PKE.** | **Uwaga uwzględniona**  Definicja komunikatu elektronicznego zostanie uspójniona z projektem ustawy - Prawo komunikacji elektronicznej. |
|  | ZTKIG | Art. 2 pkt 9 | **Art. 2 ust. 1 pkt 9**  Definicja o takiej treści znajduje się już w projekcie ustawy Prawo komunikacji elektronicznej (art. 2 pkt 35 projektu PKE).  **Jest to kolejny argument przemawiający za tym, aby regulacje objęte projektem umieścić w prawie telekomunikacyjnym lub w projektowanej ustawie PKE.** | **Uwaga wyjaśniona**  Ustawa posługuje się siatką pojęciową niezbędną dla uregulowania materii nadużyć w komunikacji elektronicznej. |
|  | ZTKIG | **Art. 2 pkt 12** | Definicja zawarta w art. 2 pkt 12 i 13 są podobne do definicji znajdującej się w art. 2 pkt 79 projektu PKE. Definicje te nieco różnią się między sobą.  Jest to również argument przemawiający za tym, aby regulacje objęte Ustawą umieścić w ustawie z 16 lipca 2004 r. Prawo telekomunikacyjne lub w projektowanej ustawie PKE. | **Uwaga wyjaśniona**  Ustawa posługuje się siatką pojęciową niezbędną dla uregulowania materii nadużyć w komunikacji elektronicznej. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 2, art. 3 | Definicje pojęć w projekcie ustawy  Analiza definicji terminów oraz definicji nadużyć w komunikacji elektronicznej wskazuje, że terminologia w projekcie ustawy wymaga dokładnej analizy oraz korekty. Sam termin „nadużycie w komunikacji elektronicznej” z art. 2 pkt 4 projektu ustawy jest niejasny i konieczne jest jego przepracowanie. Nie jest wiadome czym jest „*przeznaczenie usług telekomunikacyjnych i urządzeń telekomunikacyjnych*”, ani czym są nienależne korzyści.  W dodatku projekt ustawy w tej definicji (oraz w innych definicjach) posługuje się zwrotami i sposobem myślenia z przepisów prawa karnego, tj. do określenia działania jako nadużycia wymaga również celu lub skutku działania polegającego najczęściej na wyrządzeniu szkody lub osiągnięciu „nienależnych korzyści”. Taka filozofia jest prawidłowa przy ocenie przez organy ścigania i wymiaru sprawiedliwości zamiaru sprawcy przy określaniu karalności czynu. W przedmiotowym projekcie ustawy jest to wadliwa regulacja, gdyż wymaga od podmiotów gospodarczych oceny celu działania ich użytkownika lub partnera handlowego, do czego przedsiębiorcy z sektora ICT nie są ani uprawnieni, ani przygotowani. Przedsiębiorca telekomunikacyjny nie jest w stanie określić czy przesyłane do jego sieci SMS mają na celu spowodowanie nieświadomego rozporządzenia majątkiem użytkownika końcowego lub mają na celu wyrządzenie mu krzywdy.  Co więcej poszczególne definicje nadużyć w komunikacji elektronicznej są niejasne oraz niespójne z przepisami projektu ustawy, w tym z samą definicją nadużycia w komunikacji elektronicznej. Definicja nadużycia w komunikacji elektronicznej wymaga celu lub skutku działania w postaci wyrządzenia szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści. Tymczasem żadna z szczegółowych form nadużyć nie ma odwołania do skutku a jedynie do celu. Co więcej cele działania przy smishingu jak i przy spoofingu są znacznie szersze niż wyrządzenie szkody lub osiągnięcie korzyści. Wskazujemy, że przykładowo wymienione cele smishingu przekierowanie na stronę internetową, żądanie kontaktu telefonicznego lub instalacji oprogramowania nie muszą prowadzić do szkody.  KIKE zwraca uwagę, że:  - przepisy projektu ustawy zostały tak sformułowane, że zakazuje się świadczenia usług telekomunikacyjnych w sposób, którego skutkiem może być osiągnięcie nienależnych korzyści. Sformułowanie to jest skrajnie szerokie i KIKE wyraża wątpliwość czy projektodawca rozważył konsekwencje tej regulacji z punktu widzenia choćby regulacji telekomunikacji. Przykładowo KIKE nie ma wątpliwości, że pobieranie przez operatorów mobilnych nadmiernych opłat za zakańczanie SMSów A2P będzie stanowiło nienależne korzyści. Oznacza to, że działania operatorów mobilnych w tym zakresie naruszają przepisy prawa i tym samym nie podlegają jego ochronie. Analogicznie ocenić należy fakt korzystania z urządzeń uzyskiwania przez OPL nieuzasadnionych korzyści związanych choćby z tranzytem wewnętrznym do sieci mobilnej.  - niezrozumiałe jest także w jaki sposób możliwe jest świadczenie usług telekomunikacyjnych niezgodnie z ich przeznaczeniem. Czy było objęte intencją prawodawcy, by każde świadczenie usług telekomunikacyjnych niezgodnie z przepisami prawa będzie stanowiło nadużycie w komunikacji elektronicznej, którego skutkiem będzie np. osiągnięcie nienależnych korzyści? Przykład w tym zakresie stanowić może zawarcie w treści umowy o świadczenie usług komunikacji elektronicznej niedozwolonej klauzuli umownej. Czy w każdym takim wypadku inni przedsiębiorcy będą zobowiązani (zgodnie z treścią art. 3 ust. 2 projektu) do zapobiegania takim nadużyciom i ich zwalczania, choćby przez blokowanie ruchu przychodzącego od przedsiębiorcy naruszającego przepisy prawa?  - wątpliwości Izby budzi także zamknięty katalog podmiotów, które mogą być poszkodowane nadużyciem w komunikacji elektronicznej. W szczególności – nie obejmuje abonentów. Nie obejmuje też podmiotów trzecich, na których szkodę niekiedy podmioty dopuszczają się nadużyć w komunikacji elektronicznej.  - przepis obejmuje w zakresie swoje dyspozycji osiągnięcie nienależnych korzyści w sytuacji, w której nie zostanie wyrządzona szkoda. Czy intencją było objęcie jego zakresem „zwykłej” działalności związanej z prowadzeniem marketingu bez zgody użytkownika?  Co kluczowe także zapis art. 16 odbiega od hipotezy art. 3 projektu (np. właśnie poprzez poszerzenie zakresu podmiotowego o podmioty inne niż wskazane w art. 3 ust. 1 pkt 1). Innymi słowy – kary przewidziane są w przypadkach, które nie są objęte zakazem opisanym w art. 3 ust. 1-3.  KIKE wyraża także zastrzeżenia wobec zakresu przedmiotowego regulacji. W szczególności niezrozumiałe jest zdefiniowanie nadużyć jako dokonywanych w komunikacji elektronicznej, mających za przedmiot komunikaty elektroniczne, podczas gdy podmiotem regulacji są wyłącznie przedsiębiorcy telekomunikacyjni, tj. podmioty inne niż podmioty świadczące usługi komunikacji interpersonalnej niewykorzystujące numerów, w szczególności dostawcy poczty elektronicznej. Niezrozumiałe jest także, dlaczego przedmiot regulacji obejmują wyłącznie wiadomości SMS, nie zaś wiadomości MMS czy RCS, nie wspominając o innych formach komunikatów niepowiązanych z sieciami. | **Uwaga częściowo uwzględniona w zakresie uzupełnienia regulacji o MMS** Ustawa będzie odnosić się do wiadomości MMS, w kontekście uprawnienia przedsiębiorcy telekomunikacyjnego do blokowania MMS, które będą zawierające treści wyczerpujące znamiona smishingu, a także w kontekście penalizowania wysyłki takich wiadomości.  **Uwaga nieuwzględniona w pozostałym zakresie**  Nie jest konieczne definiowanie każdego wyrazu wykorzystywanego w przepisach. Pojęcia takie jak przeznaczenie usług i urządzeń telekomunikacyjnych są zrozumiałe, a ich definiowanie mogłoby jedynie wprowadzić niepotrzebne wątpliwości. Ponadto, „odbiorcą”, wobec którego jest skierowane nadużycie, często będzie „abonent” w przypadku usług świadczonych na rynku detalicznym.  Równocześnie nie wydaje się właściwe stworzenie definicji spoofingu czy smishingu nie wskazując na konkretny cel jaki przyświeca sprawcy. Zgodnie z informacjami przedstawionymi przez przedsiębiorców telekomunikacyjnych oraz uwzględniając projektowane rozwiązania, możliwe będzie rozpoznawanie występowania nadużyć telekomunikacyjnych. Nie można też zgodzić się z zarzutem niespójności. Wszystkie definicje odnoszą się do celu działań sprawcy. Należy też podkreślić, że nie jest intencją projektodawcy objęcie zakresem niniejszej ustawy „zwykłej” działalności związanej z prowadzeniem marketingu bez zgody użytkownika. Wskazane przez zgłaszającego uwagę rozwiązania, w kontekście rozszerzenia obowiązków po stronie przedsiębiorców telekomunikacyjnych wiązałoby się z koniecznością analizowania treści komunikatów oraz zestawiania ich z innymi informacjami. Ponadto część komunikacji elektronicznej wykorzystuje szyfrowania end-to-end, więc wykrywanie ich byłoby niemożliwe.  Problem smishingu jest nadal aktualny istnieje, zgodnie z danymi CSIRT NASK przekazanymi przez odbiorców wiadomości:  - Łączna liczba podejrzanych SMS-ów – IV-XII 2021: 16 724;  - Łączna liczba podejrzanych SMS-ów – 1. półrocze 2022: 66 385;  - Liczba SMS-ów zawierających niebezpieczny link – IV-XII 2021: 7 313;  - Liczba SMS-ów zawierających niebezpieczny link – 1. półrocze 2022: 27 217. |
|  | HACK&PHACK DEFENCE LTD Piotr Marcin Wierzbicki | art. 2, art. 3 | UWAGA ZGŁOSZONA W RAMACH ZGŁOSZENIA LOBBINGOWEGO  Opierając się na doświadczeniu wynikającym z praktyki wnoszę o uwzględnienie moich poniższych uwag do projektu UD402:  z art. 2 ustęp 4 usunięcie słów: „celem lub skutkiem„ a w ich miejsce wpisanie słów ”skutkiem wynikającym z celowego działania”, bo znając zasadę rozliczeń między operatorskich IC/CW mogą się często zdarzać sytuacje gdy np. pracownicy jakiej bądź firmy lub nawet osoby prywatne korzystając ze swojego numeru telefonu będą w większości wykonywać połączenia wychodzące do innych sieci (np. kontakt z klientami albo starszą osobą która nie potrafi zbytnio korzystać z telefonu i ogranicza jego użytkowanie do odbierania połączeń do Niej przychodzących) a mając abonament typu No Limit przy określonych dyrektywą UE stawkach MTR/FTR - zostanie to uznane za działanie na szkodę przedsiębiorcy telekomunikacyjnego i będzie podlegać odpowiedzialności wynikającej z niniejszego projektu ustawy.  Do tego słowa „osiągnięcie nienależytych korzyści” art. 2 ustęp 4 w w/w przypadkach można przypisać operatorowi telekomunikacyjnemu do którego sieci byłyby takie połączenia kierowane i także pociągnąć do odpowiedzialności z mocy niniejszej ustawy dlatego wnoszę o skreślenie słów ”lub osiągnięcie nienależytych korzyści”.  Dlatego wnoszę o wycofanie się z penalizacji i wszelkich innych form karania za – jak sam Ustawodawca podnosi - otwartą definicję nadużycia w komunikacji elektronicznej przez skreślenie z projektu UD402 zapisów artykułu 3 ustęp 1 pkt 1 - lub dodanie w nim w treści „**ultrakrótkich** połączeń głosowych” zamiast „połączeń głosowych”, w przypadku niezmodyfikowania tego artykułu wnoszę o jego skreślenie.  Ponadto wnoszę o skreślenie art. 16 ustęp 1 pkt 1, bo penalizuje standardową procedurę uruchamiania punktu styku sieci operatorów telekomunikacyjnych polegającą na kalibracji systemów rozliczeniowych tych operatorów.  Należy zwrócić uwagę, że istniejące przepisy Kodeksu Karnego skutecznie chronią interes prawny poszkodowanych, w tym przedsiębiorców telekomunikacyjnych oraz abonentów końcowych.  Natomiast skupiłbym się na artykułach dotyczących CLI SPOOFING oraz SMISHING bo nie wzbudzają one większych kontrowersji poza oczywistym faktem , że np. zapoznanie się (nawet automatyczne) z treścią np. SMS wysyłanego przez adwokata narusza tajemnicę adwokacką (art 14 ustęp 2 projektu UD402 oraz art 14 ustęp 3 pkt 1 tego projektu). | **Uwaga nieuwzględniona**  Nie jest jasne dlaczego wykonywanie połączeń do klientów w sposób wskazany w uwadze miałoby mieć charakter nadużycia w komunikacji elektronicznej.  Nie jest jasne proponowane pojęcie *ultrakrótkich* połączeń głosowych.  Procedura uruchamiania punktu styku sieci operatorów telekomunikacyjnych polegająca na kalibracji systemów rozliczeniowych tych operatorów nie będzie karana, jeżeli nie będzie wypełniała znamion przestępstwa. Sytuacje te uwzględniają postanowienia umów międzyoperatorskich. |
|  | IAB Polska | 5 | **UWAGA:**  Zdaniem IAB Polska definicja nadużycia w komunikacji elektronicznej jest niepełna, ponieważ nie uwzględnia sytuacji, gdy nie tylko świadczenie usługi telekomunikacyjnej może stanowić nadużycie w komunikacji elektronicznej, ale również korzystanie z usług telekomunikacyjnym może takie nadużycie stanowić, zwłaszcza że definicja nadużycia telekomunikacyjnego (art. 2 pkt 26) PKE) wskazuje, że nadużyciem jest „*świadczenie lub korzystanie z usługi telekomunikacyjnej*”.  **PROPOZYCJA:**  IAB Polska proponuje następującą zmianę definicji nadużycia w komunikacji elektronicznej:  *4) nadużycie w komunikacji elektronicznej – 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 końcowemu lub osiągnięcie nienależnych korzyści;* | **Uwaga uwzględniona**  Definicja nadużycia w komunikacji elektronicznej zostanie uzupełniona o aspekt „korzystania”. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 2 ust. 4 | **Definicja nadużycia w komunikacji elektronicznej** (art. 2 pkt 4 projektu ustawy)  Uzupełnienia o aspekt „korzystania” z usług telekomunikacyjnych wymaga projektowana definicja „nadużycia w komunikacji elektronicznej” (art. 2 pkt 4) projektowanej ustawy). Bez wątpienia projektowana definicja jest wzorowana na definicji „nadużycia telekomunikacyjnego”, zwartej w art. 2 pkt 26) projektu ustawy – Prawo komunikacji elektronicznej (dalej „projekt PKE”), jednak z powodów których nie znamy definicja tego pojęcia na gruncie projektu ustawy pomija element „korzystania” z usług telekomunikacyjnych jako działanie składające się na nadużycie. W naszej ocenie zawarta w projektowanej ustawie definicja „nadużycia w komunikacji elektronicznej” powinna, na wzór projektu PKE, uzyskać następujące brzmienie:  *nadużycie w komunikacji elektronicznej - świadczenie lub korzystanie z usługi telekomunikacyjnej lub urządzeń telekomunikacyjnych niezgodnie z ich przeznaczeniem lub przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;*  Pominięcie „korzystania” z usług telekomunikacyjnych na poziomie definicji oznaczałaby diametralne zawężenie przypadków kwalifikujących się jako „nadużycie w komunikacji elektronicznej” w rozumieniu projektowanej ustawy, gdyż wiele nadużyć polega na korzystaniu z usług telekomunikacyjnych w sposób niezgodny z przepisami prawa i ich przeznaczeniem. Jedynie tytułem przykładu smishing (SMS) czy sztuczny ruch – a więc zjawiska wprost wskazane w projekcie ustawy jako nazwane postacie nadużyć w komunikacji elektronicznej (art. 3 ust. 1 projektu ustawy) - to przypadki korzystania z usług telekomunikacyjnych w sposób niezgodny z przepisami prawa i ich przeznaczeniem. Zatem należy powrócić do pierwotnego brzmienia definicji. | **Uwaga uwzględniona**  Definicja nadużycia w komunikacji elektronicznej zostanie uzupełniona o aspekt „korzystania”. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 2 pkt 4 | **IX. [DEFINICJA NADUŻYCIA W KOMUNIKACJI ELEKTRONICZNEJ – ART. 2 PKT 4)]**  **(33.)** W naszej ocenie pojęcie „*niezgodnego z ich przeznaczeniem*” wykorzystywania usługi jest zbyt nieostre, by mogło stanowić podstawę do jakichkolwiek sankcji.  **(34.)** Jeszcze raz pragniemy odnieść się do Prezentacji, gdzie podkreślono, że „*definicja posługuje się nieostrymi pojęciami, brak jest wyraźnie stypizowanych i konkretnych zachowań kwalifikujących je jako nadużycie telekomunikacyjne (może z wyjątkiem „nieuprawnionej” modyfikacji informacji adresowej o numerze)*”.  **(35.)** Wnosimy zatem o usunięcie z definicji [art. 2 pkt 4)] passusu „*z ich przeznaczeniem lub*”.  W konsekwencji art. 2 pkt 4) Projektu powinien otrzymać następujące brzmienie:  „*nadużycie w komunikacji elektronicznej – świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych niezgodnie przepisami prawa, których celem lub skutkiem jest wyrządzenie szkody przedsiębiorcy telekomunikacyjnemu, użytkownikowi końcowemu lub osiągnięcie nienależnych korzyści;”* | **Uwaga nieuwzględniona**  Nadużycia w komunikacji elektronicznej mają zgoła różny i często skomplikowany charakter dlatego celowo definicja jest ogólna.  Świadczenie usługi telekomunikacyjnej niezgodnie z jej przeznaczeniem również powinno być uznane za nadużycie w komunikacji elektronicznej (por. art. 5 Kodeksu cywilnego). |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 2 pkt 8 | **ad Art. 2 pkt 8)** poczta elektroniczna – usługę komunikacji interpersonalnej niewykorzystującą numerów, która umożliwia przekazywanie komunikatu elektronicznego z wykorzystaniem standardu SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol), lub IMAP4 (Internet Message Access Protocol);  Propozycja PTI  Powyższą definicję skrócić do postaci:  *poczta elektroniczna – usługa przekazywania komunikatu elektronicznego z wykorzystaniem protokołu SMTP bądź protokołów będących jego rozszerzeniem.*  Komentarz PTI  W treści ustawy nie należy umieszczać nazw produktów/protokołów, które mogą się z czasem technicznie zmieniać i występować pod innymi nazwami – wystarczy podać jedynie charakterystyczny protokół SMTP z ogólnym dopuszczeniem protokołów go rozszerzających. Fraza *...komunikacji interpersonalnej niewykorzystującą numerów, …* jest niepotrzebna. | **Uwaga nieuwzględniona**  Poczta e-mail jest usługą komunikacji interpersonalnej niewykorzystującą numerów. Wskazanie wyłącznie standardu SMTP w nieuzasadniony sposób utrudni właściwą subsumpcję normy prawnej. |
|  | Unia Metropolii Polskich | Art. 2 pkt 8 | Definicja poczty elektronicznej jest zbyt wąska i kazuistyczna. Nie obejmuje m.in. protokołów np. Exchange ActiveSync Microsoftu. Definicję należy zmienić na bardziej opisową . | **Uwaga uwzględniona**  Poprzez dodanie „lub innego standardu zapewniającego te same funkcje”. |
|  | IAB Polska | Art. 2 pkt 12 | **UWAGA:**  Przez wzgląd na rosnącą jakością obsługi konsumenta coraz powszechniejsze staje się udostępnianie na stronach internetowych świadczących różnego rodzaju usługi (sklepy internetowe, platformy handlu elektronicznego, platformy gier internetowych czy inne) dedykowanych kanałów ułatwiających komunikację konsumenta korzystającego z usług elektronicznych ze sprzedającym bądź z innymi użytkownikami danej strony. Przykładem takich narzędzi do komunikacji interpersonalnej niewykorzystującej numerów stanowią chatboty czy dedykowane kanały komunikacji. Usługa ta pozostaje podrzędna i dodatkowa względem usługi głównej, tj. przykładowo, sprzedaży przez stronę internetową bądź pośrednictwa w sprzedaży na platformie.  Wyłączenie zawarte w art. 2 pkt 12 projektowanej ustawy ujęte zostało w sposób bardzo ogólny. Biorąc pod uwagę, iż zakres wyłączenia nie został doprecyzowany ani określony w uzasadnieniu do projektu ustawy, zakres podmiotowy projektowanej ustawy pozostaje niepewny, co w naszej ocenie może rodzić wątpliwości interpretacyjne kiedy regulacja wejdzie już w życie. Sankcyjny charakter projektowanej regulacji w połączeniu z terminologiczną niepewnością ma duży potencjał wywołania tzw. *chilling effect* wśród legalnie i prawidłowo działających podmiotów, a ponadto w takiej formule wywołuje uzasadnione zastrzeżenia odnośnie konstytucyjności takiej formuły zakazu i zgodności z prawidłową techniką prawodawczą.  **PROPOZYCJA:**  Nałożenie określonych w projektowanej ustawie obowiązków na przedsiębiorców prowadzących sklepy internetowe, będących operatorem platformy handlu elektronicznego czy portali udostępniających gry internetowe, którzy udostępniają kanały komunikacji stanowiącę usługę komunikacji interpersonalnej niewykorzystującej numerów byłoby nieproporcjonalne do świadczonych przez nich usług.  W związku z powyższym proponujemy dodanie zdania drugiego do obecnego brzmienia art. 2 pkt 12 w następujący sposób “(...) *Funkcję podrzędną względem usługi podstawowej stanowi w szczególności usługa komunikacji interpersonalnej udostępniona w sklepach internetowych, na platformach handlu elektronicznego czy w grach internetowych.*”, bądź dodanie do uzasadnienia projektu ustawy powyższego zdania. | **Uwaga nieuwzględniona**  Projekt ustawy nie reguluje obowiązków operatorów platform handlu elektronicznego czy portali udostepniających gry internetowe. Uwaga jest to poza zakresem projektowanej ustawy. |
|  | Związek Banków Polskich | Art. 2 pkt 17 i 18 | **17) bank – podmiot, o którym mowa w art. 2 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.),**  **18) spółdzielcza kasa oszczędnościowo-kredytowa – podmiot, o którym mowa w art. 2** **ustawy z dnia 5 listopada 2009 r. o spółdzielczych kasach oszczędnościowo-kredytowych (Dz.U. 2022 r. poz. 924).**  Proponujemy wprowadzenie definicji pojęć użytych w projekcie ustawy. | **Uwaga częściowo uwzględniona**  Odwołania do definicji ustawowych banku i SKOK znajdą się w przepisach dotyczących listy numerów wykorzystywanych wyłącznie do odbierania połączeń. |
|  | Polska Wytwórnia Papierów Wartościowych | Art. 3 ust. 1 | W art. 3 ust. 1 projektu ustawy ujęto opisowo rodzaje nadużyć spotykanych w komunikacji elektronicznej, każdorazowo opatrując dane zachowanie nawiasem wraz z używaną nazwą, takich jak „sztuczny ruch”, „smishing” czy „CLI spoofing”. W związku z tym, że te pojęcia nie są powszechnie znane proponujemy rozważenie umieszczenia definicji w art. 2 projektu ustawy. | **Uwaga nieuwzględniona**  Celowo wyodrębniono konkretne nadużycia w komunikacji elektronicznej. Zgodnie z zasadą zwięzłości tekstu prawnego przyjęte w projekcie rozwiązanie jest bardziej adekwatne. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 3 ust. 1 pkt 1 | Sztuczne generowanie ruchu  *„inicjowanie wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej , lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch)”*  Izba potwierdza, że to nadużycie było wcześniej problemem związanym z wysokimi stawkami rozliczeniowymi między przedsiębiorcami telekomunikacyjnymi. Obecnie z powodu zmniejszenia w rozporządzeniu unijnym stawek FTR i MTR problem ten ma znacznie mniejszą skalę i szkody.  W dodatku projekt ustawy oprócz zdefiniowania tego zjawiska (nieprecyzyjnego i niejasnego) nie wprowadza żadnych regulacji związanych z tym nadużyciem. Jednocześnie Izba wskazuje, że przedsiębiorcy telekomunikacyjni (przy współpracy Prezesa UKE) pozwierali umowy międzyoperatorskie identyfikujące i zwalczające to nadużycie. Wprowadzenie tej regulacji w ustawie spowoduje konieczność zmiany tych umów międzyoperatorskich i kolejną dyskusję na temat legalności określonych rodzajów połączeń. Przykładowo Izba wskazuje, że istotą sztucznego ruchu jest wygenerowanie określonych „połączeń” w systemach billingowych. Nie jest celem sztucznego ruchu wyłącznie zarejestrowanie się na punktach styku sieci, gdzie rejestrowane są połączenia odebrane jak i nie odebrane (tylko te pierwsze generują przychody z rozliczeń międzyoperatorskich). Co więcej, proponowana definicja sztucznego ruchu obejmie połączenia testowe wykorzystywane przez przedsiębiorców telekomunikacyjnych do wykrywania spoofingu (operator generuje połączenia z danego kierunku co do którego ma podejrzenia podmieniania numeracji, po czym weryfikuje z jakim numerem to połączenie wróciło do jego sieci).  W opinii Izby w chwili obecnej nie ma powodu do ustawowej regulacji sztucznego ruchu, tym bardziej że głównymi podmiotami dokonującymi takich działań są podmioty zagraniczne, których projekt ustawy nie obejmuje. | **Uwaga nieuwzględniona**  Nadużycie związane ze sztucznym ruchem powinno być wprost zakazane na podstawie przepisów ustawy. W przypadku zagadnień mogących budzić jakąkolwiek wątpliwość (jak np. połączenia testowe), są przesądzone na gruncie umów zawieranych pomiędzy przedsiębiorcami. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 3 ust. 1 pkt 1 | ad Art. 3. ust. **1. pkt 1)** inicjowania wysyłania lub odbierania komunikatów elektronicznych lub połączeń głosowych w sieci telekomunikacyjnej z wykorzystaniem urządzeń telekomunikacyjnych lub programów, których celem nie jest skorzystanie z usługi telekomunikacyjnej, lecz ich zarejestrowanie na punkcie połączenia sieci telekomunikacyjnych bądź przez systemy rozliczeniowe (sztuczny ruch);  Propozycja PTI  Usunąć frazę  *...lub odbierania….*  Komentarz PTI  Wpisanie frazy *...lub odbierania….* nie ma uzasadnienia, gdyż odbiorca takich komunikatów elektronicznych nie ma wpływu (oprócz całkowitej blokady dostępu do wszystkich komunikatów) na ich odbieranie. Jedynie po rozpoznaniu, mając odpowiednią wiedzę lub doświadczenie, może je zakończyć lub usunąć. W żadnym stopniu nie może odpowiadać za ich rozpowszechnianie, jeżeli ich dalej nie rozsyła, pod warunkiem że ma wiedzę, że są one komunikatami szalbierskimi. | **Uwaga nieuwzględniona**  Ruch ten może być wprowadzany do sieci telekomunikacyjnej, niekoniecznie „inicjowany”, aby działanie takie stanowiło nadużycie polegające na sztucznym ruchu. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 3 ust 1 pkt 1 | **Art. 3 ust. 1 pkt 1**  Pomysł, aby działalność w zakresie tzw. sztucznego ruchu traktować jako nadużycie należy ocenić pozytywnie. Natomiast wydaje się bardzo trudne (jeśli w ogóle możliwe) do wykazania, że dane zdarzenie ma znamiona nadużycia.  Argumentem przemawiającym za stwierdzeniem, że określone działanie jest nadużyciem, jest cel tego działania, nawet w przypadku, gdy to działanie nie wywoła jakichkolwiek skutków.  Celem bowiem przepisów projektu jest stworzenie narządzi do zapobiegania nadużyciom w komunikacji elektronicznej zanim wywołają skutki.  W projekcie nie określono sposobu zapobiegania nadużyciom w komunikacji elektronicznej zdefiniowanych w art. 3 ust. 1 pkt 1 projektu, ani też nie wskazano podmiotów i ich obowiązków w tym zakresie.  Ponadto brak jest definicji pojęć: „*punkt połączenia sieci telekomunikacyjnych*”, „*systemy rozliczeniowe*”. Również prawo telekomunikacyjne nie definiuje takich pojąć.  **Postulować by zatem wypadało umieszczenie w słowniczku ustawowym pojęć: „*punkt połączenia sieci telekomunikacyjnych*”, „*systemy rozliczeniowe*” oraz określenie ich definicji legalnych.** | **Uwaga wyjaśniona**  Pod pojęciem systemów rozliczeniowych należy rozumieć każdy system używany przez przedsiębiorcę telekomunikacyjnego do obsługi rozliczeń za usługi telekomunikacyjne.  Punkt styku sieci, czy punkt połączenia sieci telekomunikacyjnych należy intepretować zgodnie z przepisami ustawy Prawo telekomunikacyjne. W przypadku innych wyrażeń i wątpliwości – ze słownictwem używanym w dziedzinie telekomunikacji. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 3 ust. 1 pkt 2 | **ad Art. 3 ust. 1. pkt 2)** wysyłania krótkich wiadomości tekstowych (SMS), w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę internetową, żądania kontaktu telefonicznego lub instalacji oprogramowania (smishing);  Propozycja PTI  W danym przepisie i w całym tekście ustawy używanie terminu **esemes** (zamiast SMS) oraz nazwanie tych komunikatów terminem **esemesy szalbierskie**.  Komentarz PTI  Rozwinięcie jest zawarte w uwadze ogólnej. | **Uwaga nieuwzględniona**  Określenie „szalbierczy” potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, iż jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach. Z tego powodu proponuje się pozostawienie pojęcia „smishing”, które jest powszechnie znane i wykorzystywane. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 3 ust. 1 pkt 3 | Spoofing  *„nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing)”.*  Izba całkowicie zgadza się z Panem Ministrem w konieczności bezprawnej podmiany numeru wywołującego połączenie telefoniczne. Niemniej wskazujemy, że definicja tego zjawiska w projekcie ustawy jest niejasna oraz niepełna. Nie obejmuje ona wiele niekorzystnych zjawisk związanych z podmianą numeru abonenta (fraudy na rozliczeniach międzyoperatorskich, ukrywanie przez służbami numeru, z którego wykonywane są fałszywe alarmy bombowe). Do regulacji wymaga ona podszywania się pod inny podmiot oraz określonego celu działania oszusta, który nie musi być wiadomy przedsiębiorcy telekomunikacyjnemu. Definicja nie obejmuje m.in. podmiany numeru A w zakresie zmiany rozliczeń za zakańczanie połączeń czy w celu wyłudzenia danych bankowych. | **Wyjaśnienie**  Kwestia oszustw na rozliczeniach międzyoperatorskich została uwzględniona w definicji sztucznego ruchu. Z kolei kwestia wyłudzania danych bankowych jest uwzględniona w obecnej definicji spoofingu. W związku z tym, że wprowadzone zostało nadużycie w telekomunikacji polegające na nieuprawnionej modyfikacji informacji adresowej w postaci numeru telefonu lub identyfikatora użytkownika wysyłającego komunikat elektroniczny albo wywołującego połączenie głosowe. Tym samym ukrywanie numeru przed służbami również będzie ujęte w tej ustawie. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 3 ust. 1 pkt 3 | **Definicja CLI spoofingu** (art. 3 ust. 1 pkt 3) projektu ustawy)  Przedstawiona w projekcie ustawy definicja zakłada, że CLI spoofing ma miejsce w przypadku, gdy nieuprawnionego posłużenia się informacją adresową dopuszcza się „użytkownik” wywołujący połączenie głosowe. I faktycznie tak skonstruowana definicja obejmie swoim zakresem zdecydowaną większość przypadków CLI spoofingu. Niemniej jednak pogłębione analizy wykazały, że historycznie zdarzały się (nieliczne, ale jednak) przypadki, w których podmiotem w sposób nieuprawniony posługującym się informacją adresową podczas inicjowania połączenia był nieuczciwy przedsiębiorca telekomunikacyjny (a nie użytkownik). Biorąc pod uwagę, że pojęcie „użytkownika” jest zdefiniowane w ustawie – Prawo telekomunikacyjne (i oznacza podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi – art. 2 pkt 49) ustawy – Prawo telekomunikacyjne) tak skonstruowana definicja CLI spoofingu będzie pomijała przypadki, w których to nieuczciwy przedsiębiorca telekomunikacyjny jest podmiotem, który inicjuje połączenie w sposób nieuprawniony posługując się informacją adresową.  Ponadto, zwracamy uwagę, że przedsiębiorcy telekomunikacyjni nie dysponują i nie będą dysponowali rozwiązaniami, które pozwolą ustalić jaki cel ma osoba albo podmiot wykonujący spoofowane połączenie głosowe. Z perspektywy organów ścigania tak skonstruowana definicja będzie oznaczała konieczność udowodnienia, że sprawca działał w celu nakłonienia odbiorcy połączenia do określonego działania, co dowodowo może być trudne do osiągnięcia. Nie można również zapominać, że w niektórych przypadkach, znanych publicznie i opisywanych w mediach, celem sprawców nie było nakłonienie ofiary do określonego działania, a sprawcom chodziło najprawdopodobniej o wywołanie strachu, poczucia zagrożenia u odbiorcy spoofowanego połączenia (przypadki osób publicznych i polityków otrzymujących połączenia informujące o śmierci osób najbliższych). Z tej perspektywy warto się zastanowić nad usunięciem z definicji słów „… służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania …”.  W związku z powyższym, aby definicja CLI spoofingu obejmowała wszystkie znane scenariusze działań nadużyciowych w tym zakresie, postulujemy nadanie jej następującego brzmienia (zmiany w stosunku do obecnego brzmienia przepisu widoczne są jako przekreślenia i podkreślenia):  *nieuprawnionego posłużenia się przez ~~użytkownika~~ wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ~~ten użytkownik~~ podmiot wywołujący~~, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania~~ (CLI spoofing).*  Definicja w kształcie zaproponowanym powyżej powinna objąć swoim zakresem wszystkie znane przypadki CLI spoofingu, a zaproponowane brzmienie usuwa potencjalne problemy jakie wiążą się z niemożnością ustalenia przez przedsiębiorcę telekomunikacyjnego zamiaru / celu / intencji spoofera, ułatwiając organom ścigania pociągniecie sprawców do odpowiedzialności, zwalniając je z konieczności udowodnienia działania w konkretnym celu. Jednocześnie definicja w zaproponowanym brzmieniu zachowuje podstawowe przesłanki uznania określonego działania za CLI spoofing, mianowicie nieuprawnione posłużenie się informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż podmiot wywołujący połączenie głosowe.  W przypadku uwzględnienia powyższych zmian definicyjnych odpowiednich zmian wymagać będzie również brzmienie art. 16 ust. 1 pkt 3) projektu ustawy. | **Uwaga uwzględniona częściowo**  W definicji CLI spoofing zostanie dodane, że może się go dopuścić również przedsiębiorca telekomunikacyjny. W definicji zostanie uwzględniona również intencja w postaci wywołania strachu u innej osoby.  **W pozostałym zakresie uwaga nieuwzględniona**  Nie można zgodzić się z usunięciem z definicji CLI spoofingu intencji sprawcy. Celem ustawy jest przeciwdziałanie konkretnym przestępstwem i działanie w tym zakresie muszą odnosić się do tych działań. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 3 ust. 1 pkt 3 | **ad Art. 3 ust. 1 pkt 3)** nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).  Propozycja PTI  Wprowadzenie zamiast określenia „(CLI spoofing)” terminu:  ***szalbierczy numer dzwoniącego***  Komentarz PTI  Termin CLI spoofing jest mało zrozumiały. Już lepszy byłby termin Caller ID spoofing, gdyby nie był angielski, dlatego proponujemy używanie terminu - **szalbierczy numer dzwoniącego,** jednoznacznie wskazujący na szkodliwy identyfikator dzwoniącego. | **Uwaga nieuwzględniona**  Określenie „szalbierczy” potwierdza bogactwo języka polskiego. Nie da się jednak nie zauważyć, iż jest to archaizm. Wyraz ten jest rzadko używany w codziennych dyskursach. Z tego powodu proponuje się pozostawienie pojęcia „smishing”, które jest powszechnie znane i wykorzystywane. |
|  | Polska Izba Komunikacji Elektronicznej | Art. 3 ust. 1 pkt 3 | **Pojęcie „CLI spoofing” *(art. 3 ust. 1 pkt 3)***  Art. 3 ustawy wprowadza katalog otwarty nadużyć w komunikacji elektronicznej. Jednocześnie wskazuje na trzy typowe naruszenia, stanowiące największe zagrożenia.  PIKE szczególnie zwraca uwagę na proponowane w art. 3 ust. 1 pkt 3) pojęcie CLI spoofing.  Proponuje się, aby przepis przyjął następujące brzmienie:  **Art. 3.** 1. Zakazane są nadużycia w komunikacji elektronicznej, w szczególności dotyczące:  (…)  3) nieuprawnionego posłużenia się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).  Otóż zawarte w projekcie pojęcie CLI spoofing nie zostało dostatecznie doprecyzowane. Nie uwzględnia ono szeregu stosowanych obecnie technologii i występujących zjawisk, a także odmiennych niż wskazane w przepisie działań użytkownika. Za przykład może posłużyć wskazane już wcześniej zjawisko podmiany numeru abonenta, z którego dokonywane jest połączenie. Co więcej, wskazuje się, że jest to działanie służące podszyciu się pod inny podmiot, a zatem skoro użytkownik podawałby się za podmiot nieistniejący, to nie wkraczałoby to w zakres zastosowania przepisu (błąd legislacyjny).  Zastosowanie przepisu zostało w ten sposób znacznie zawężone. Egzekwowanie regulacji i objęcie nią możliwie wielu odmian spoofingu wymaga przygotowania pojęcia udoskonalonego, precyzyjnego i uwzględniającego szeroki wachlarz stosowanych technologii i działań. **Izba postuluje zatem o podjęcie próby zaprojektowania definicji od początku.** | **Uwaga częściowo uwzględniona**  W projekcie zostanie dodana nowa postać nadużycia w komunikacji elektronicznej, uwzględniające podmianę numeru abonenta. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 3 ust. 1 pkt 3 | **Art. 3 ust. 1 pkt 3**  Pojęcie „informacja adresowa” jest niejednoznaczne.  **Proponujemy zatem zawarcie definicji legalnej tego pojęcia w słowniczku projektu.** | **Uwaga nieuwzględniona**  Pojęcie to nie jest definiowane również w Prawie telekomunikacyjnym oraz w projektowanym Prawie komunikacji elektronicznej, podobnie jak inne zwroty dotyczące kwestii identyfikacji użytkownika. Przepisy powinny być przyszłościowe, a samo pojęcie informacji adresowej jest bardzo pojemne - obejmuje numery i identyfikator użytkownika. Identyfikatorem mogą być znaki identyfikujące abonenta (z art. 130 Pt np. adresy elektroniczne, nazwy, kody, radioamatorskie znaki identyfikujące stację) oraz też adresy IP. W powyższym zakresie zostało uzupełnione uzasadnienie. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 3 ust. 1 | II. [OTWARTOŚĆ KATALOGU NADUŻYĆ – ART. 3 UST. 1]  **(3.)** Zwracamy uwagę, że **określenie otwartego katalogu** zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej **nie jest zasadne**.  **(4.)** Wskazujemy, że penalizowane są jedynie nadużycia enumeratywnie określone w art. 3 ust. 1 pkt 1-3.  **(5.)** Zatem z praktycznego punktu widzenia **ogólny zakaz nadużyć w komunikacji elektronicznej okaże się nieskuteczny**.  **(6.)** W tym zakresie zwracamy uwagę, że w 2018 r. ówczesne MC wskazało (w odpowiedzi na uwagi zgłaszane przez PIIT i KIGEiT w ramach tzw. Okrągłego Stołu ds. FTR w prezentacji zatytułowanej „*NADUŻYCIA TELEKOMUNIKACYJNE – PROPOZYCJE IZB*”; prezentacja została przesłana w dniu 10 września 2018 r., zwana dalej „***Prezentacją***”), że „*wydaje się, że tego rodzaju działania powinny być precyzyjnie wskazane, zwłaszcza że podlegać mają sankcjonowaniu przez organ regulacyjny*” (Prezentacja s. 3).  Zdaniem Izby powyższe wątpliwości są aktualne.  **(7.)** Naszym zdaniem należy **rozważyć rozszerzenie katalogu zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej oraz jego zamknięcie**.  Zatem **w art. 3 ust 1 wnosimy o usunięcie zwrotu „w szczególności”**. | **Uwagi nieuwzględnione**  Problem nadużyć nie ogranicza się wyłącznie do zjawisk sztucznego ruchu, smishingu, CLI spoofingu i podszywania się w komunikacji z wykorzystaniem poczty elektronicznej. Nie należy również zakładać, że nie jest zmienny w czasie. Dlatego zasadne jest odzwierciedlenie stanu faktycznego poprzez otwarcie katalogu. Nie mniej, ze względu na fakt, ze pozostałe nadużycia są „nienazwanymi” w świetle projektu ustawy, obowiązek przeciwdziałaniu nim nie jest obwarowany sankcjami. Równocześnie jednak przedsiębiorcy telekomunikacyjni powinni podejmować działania mające przeciwdziałać nowym metodom działania przestępców. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 3 ust. 1 | **[ROZSZERZENIE NAZWANYCH PRZYPADKÓW NADUŻYĆ W KOMUNIKACJI ELEKTRONICZNEJ – ART. 3 UST. 1]**  **(8.)** Izba od wielu lat wskazuje, że **genezą większości nadużyć jest podmiana numeru A (czego emanacją jest również CLI spoofing) oraz korzystanie z usług detalicznych w celu realizacji usług hurtowych**.  **(9.)** Istotą nadużycia w zakresie podmiany numeru jest to, że (z uwagi na asymetrię rozliczeń EOG/non-EOG) połączenia kierowane z obszaru non-EOG są opisywane numerami ze strefy EOG (w tym numerami krajowymi).  Celowa modyfikacja przez nieuczciwych przedsiębiorców numeru międzynarodowego na numer krajowy w systemach bilingowych, prowadzi do stosowania w rozliczeniach międzyoperatorskich niższej stawki.  Dodatkowo należy podkreślić, iż propozycje regulacji dotyczące niezmienności numeru będą miały na względzie zapewnienie bezpieczeństwa i porządku publicznego, co sprzyjać będzie prawidłowemu wykonywaniu obowiązków przez organy powołane m.in. do niesienia pomocy (lokalizacja).  **(10.) Wnosimy stąd o uzupełnienie zachowań wyczerpujących znamiona nadużyć w komunikacji elektronicznej o przypadki, o których mowa w pkt (11-12.)**.  **(11.)** W stanowisku z dnia 15 października 2018 r. sformułowaliśmy następującą redakcję przepisu:  *„1. Zakazane jest nieuprawnione wykorzystanie usług telekomunikacyjnych, w połączonych sieciach lub innych sieciach telekomunikacyjnych, przy zastosowaniu środków niezgodnych z prawem, polegające na:*  *a) nieuprawnionej modyfikacji lub zmianie numeru inicjującego połączenie (numeru A), z zastrzeżeniem ust. 2,*  *b) przesyłaniu sygnalizacji niezwiązanej ze świadczeniem usług,*  *c) świadczeniu hurtowych usług międzysieciowych z wykorzystaniem usług abonenckich, w tym z wykorzystaniem urządzeń FCT, simboxing,*  *d) wykorzystaniu jakichkolwiek numerów bądź zakresów numeracji niezgodnie z ich przeznaczeniem określonym w PNK lub decyzji o przydziale numeracji.*  *2. Nie stanowi zmiany, o której mowa w ust. 1 modyfikacja numeru, która wynika z realizacji zasad adresowania dla właściwego kierowania połączeń ustalonych na podstawie art. 126 ust. 13”.*  Powyższe zachowania są aktualne obecnie.  **(12.)** Ingerencji ustawowej wymagają również inne przypadki nadużyć telekomunikacyjnych, takie jak celowe przesyłanie sygnalizacji niezwiązanej ze świadczeniem usług, świadczenie hurtowych usług międzysieciowych z wykorzystaniem usług abonenckich, w tym z wykorzystaniem urządzeń FCT, simboxing oraz wykorzystanie jakichkolwiek numerów bądź zakresów numeracji niezgodnie z ich przeznaczeniem określonym w PNK lub decyzji o przydziale numeracji.  **(13.)** Przedstawione rozwiązanie bazuje na wypracowanych na rynku telekomunikacyjnym postanowieniach umownych związanych z regulacją stawek MTR i FTR.  **(14.)** W ocenie Izby **niezbędne jest wprowadzenie sankcji w postaci pieniężnej kary administracyjnej, która będzie dodatkowo odstraszać przed stosowaniem nieuczciwych praktyk, o których mowa powyżej**.  Na szczególną uwagę zasługuje kwestia niezmienności numeru A na całej drodze połączenia. **Obecnie takiego typu zachowania nie są penalizowane, a ogólny obowiązek niezmienności adresacji na całej drodze połączenia wynika z rozporządzenia, a nie ustawy**. | **Uwaga częściowo uwzględniona w zakresie modyfikacji numeru międzynarodowego na numer krajowy**  W projekcie zostanie dodana nowa postać nadużycia w komunikacji elektronicznej, uwzględniające podmianę numeru abonenta.  Informacja adresowa o numerze abonenta wywołującego powinna być zasadniczo niezmienna na całej drodze połączeniowej, o czym stanowi obecne brzmienie § 1 załącznika pn. „Szczegółowe wymagania dotyczące zasad adresowania dla właściwego kierowania połączeń” do rozporządzenia Ministra Administracji i Cyfryzacji z dnia 12 grudnia 2014 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania połączeń dla właściwego kierowania połączeń. Dodany do projektu ustawy nowy rodzaj nadużycia polega na niedozwolonym oddziaływaniu na urządzenia telekomunikacyjne i zmianę danych rejestrowych np. połączenia międzynarodowego wywołującego (numeru A) oraz takim kierowaniu ruchu telekomunikacyjnego z/do innych sieci telekomunikacyjnych lub za pośrednictwem sieci operatorów, aby zgubić źródło ruchu i zakończyć połączenie po stawkach krajowych. Zasadniczym celem podmiany numeru jest wprowadzenie w błąd (co do źródła ruchu) systemów operatora do którego powinien trafić ruch. W wyniku powyżej opisanej działalności operatorzy telekomunikacyjni nie są w stanie przedstawić prawdziwych i kompletnych informacji o tym, kto faktycznie dzwonił na podany numer.  **W pozostałym zakresie uwaga nieuwzględniona**  W zakresie rozliczeń między operatorami należy zauważyć, że sztuczny ruch został już uwzględniony w projekcie ustawy. Pozostałe propozycje mogą się mieścić w otwartym katalogu nadużyć w komunikacji elektronicznej. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 3 ust. 2 | **V. [OBOWIĄZEK PODEJMOWANIA PROPORCJONALNYCH ŚRODKÓW TECHNICZNYCH I ORGANIZACYJNYCH MAJĄCYCH NA CELU ZAPOBIEGANIE NADUŻYCIOM W KOMUNIKACJI ELEKTRONICZNEJ I ICH ZWALCZANIE – ART. 3 UST. 2]**  **(24.)** Taki ogólny obowiązek pojawił się w niektórych propozycjach Rynku dotyczących rozwiązań legislacyjnych w zakresie zwalczania nadużyć.  **(25.)** W tym jednak zakresie należy wskazać, że **taki ogólny obowiązek nie został przez MC zaaprobowany**.  Zwracano uwagę na następujące wątpliwości:  1) „*co dzieje się w praktyce, w przypadku gdy Prezes UKE uzna, że zastosowane środki są nieproporcjonalne lub nie służą realizacji celów przepisu? Co jeśli przedsiębiorca się odwoła od decyzji Prezesa? Jak dalej wygląda postępowanie?*”;  2) „*jakie są przesłanki do dokonania oceny, czy zastosowane środki są proporcjonalne i służą realizacji celu?*”;  3) „*czy przedsiębiorca ponosi odpowiedzialność za zastosowanie środków w przypadku zakazu Prezesa UKE?*”.  Powyższe stwierdzenia pozostają aktualne.  **(26.)** Do rozważenia pozostawiamy to, aby ustalić te środki w rozporządzeniu, o którym mowa powyżej. | **Uwaga wyjaśniona**  Nadużycia w komunikacji elektronicznej mają zgoła różny i często skomplikowany charakter, a co za tym idzie przeciwdziałanie i zwalczanie ich wymaga podejmowania różnych (odmiennych) środków technicznych i organizacyjnych. Ww. jednostka redakcyjna zawiera ogólny obowiązek, dlatego mając na względzie na jego charakter, niesprostanie temu obowiązkowi – o ile nie jest związane z innymi, bardziej szczegółowymi obowiązkami – nie wiąże się z jakąkolwiek sankcją. Natomiast taka redakcja przepisu pozwala podkreślić, że projektodawca (a w przyszłości ustawodawca), nie tylko ma świadomość zjawiska i problemów wynikających z nadużyć telekomunikacyjnych, ale również uświadamia przedsiębiorców, że muszą te okoliczności uwzględnić prowadząc działalność telekomunikacyjną. W przedmiocie punktu trzeciego wątpliwość jest niezrozumiała, o jakim „zakazie Prezesa UKE” jest mowa w uwadze. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 3 ust. 2 | **Art. 3 ust. 2**  Konstruując normę prawną nakładającą na przedsiębiorcę telekomunikacyjnego podejmowanie proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie projektodawca winien był wskazać w czym ma się przejawiać przedmiotowa proporcjonalność **zastosowanych środków.**  **Proporcjonalność środków zastosowanych przez przedsiębiorcę telekomunikacyjnego winna być do czegoś odniesiona, winna w zapisie projektu znaleźć się jakaś miara wedle której oceniać będzie można czy proporcja wdrożonych środków została przez przedsiębiorcę zachowana, czy też nie.** | **Uwaga wyjaśniona**  Środki mające na celu zapobieganie nadużyciom mają być proporcjonalne - więc zależne od wielkości podmiotu, posiadanej infrastruktury czy charakteru świadczonych usług. Przy określaniu proporcjonalnych środków można posiłkować się uznanymi międzynarodowymi standardami w zakresie zarządzania ryzykiem, np. COSO II czy ISO 31000. |
|  | Związek Banków Polskich | Art. 3 ust. 2 | 2. Przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych, w tym działań o charakterze edukacyjnym**,** mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie.  Poza zobowiązaniem przedsiębiorców telekomunikacyjnych do podejmowania odpowiednich środków technicznych i organizacyjnych, uzasadnione jest również wskazanie inicjatyw edukacyjnych jako koniecznego elementu zapobiegania nadużyciom.  Analiza przypadków nadużyć finansowych do których dochodziło w przeszłości pokazuje, że odpowiedni poziom wiedzy klientów sektora telekomunikacyjnego pozwoliłyby na uniknięcie wielu, najbardziej niekorzystnych skutków nadużyć (przede wszystkim niekorzystnych skutków finansowych). | **Uwaga nieuwzględniona**  W ramach środków organizacyjnych mogą mieścić się środki również o charakterze uświadamiającym użytkowników. Natomiast działania o charakterze edukacyjnym – w przeciwieństwie do innych środków, mogą być prowadzone przez różne podmioty, nie tylko przez przedsiębiorców telekomunikacyjnych, ale również np. przez Związek Banków Polskich czy podmioty publiczne. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 4 ust. 2 | **ad Art.** **4. ust. 2.** CSIRT NASK na podstawie monitorowania, o którym mowa w ust. 1, tworzy wzorzec wiadomości wyczerpującej znamiona smishingu.  Propozycja PTI  W powyższym przepisie na jego końcu, zamiast słowa ...smishingu… :  *szalbierskiego esemsesa wraz z podaniem zarzutów go dotyczących.*  Komentarz PTI  Uważamy, iż przy każdym zablokowanym rodzaju esemesa powinny być wpisane zarzuty jego dotyczące, będące podstawą blokady. Proponowania zmiana jest związana z kolejnym przepisem z art. 5, gdyż umożliwia skuteczny sprzeciw wobec decyzji CSIRT definiującej znamiona szalbierskiego esemesa (*smishingu*). | **Uwaga nieuwzględniona**  Wzorzec będzie opracowany na podstawie szeregu różnych przykładów wiadomości o charakterze smishingu. Nie jest zasadne jeszcze wskazywanie odrębnie zarzutów w stosunku do wiadomości, która w zależności od kodowania ma 160 lub 70 znaków. Proponowane rozwiązanie jest nieadekwatne. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 4-6 | Smishing  KIKE aktywnie wspiera propozycję monitorowania przez CSIRT NASK smishingu oraz tworzenie wzorców SMS zawierających smishing. Zwracamy jednak uwagę na kilka kwestii wymagających poprawy. Po pierwsze, przedsiębiorcy telekomunikacyjni oraz podmioty inicjujące wysyłanie SMSów A2P (integratorzy usług SMS A2P) powinni być uprawnieni do zgłaszania do CSIRT NASK SMS ze smishingiem do tworzenia wykazu wzorców w art. 4 projektowanej ustawy. Z doświadczenia członków Izby wynika, że to podmioty wysyłające SMS (przedsiębiorcy telekomunikacyjni i integratorzy SMS) szybciej wyłapują smishing niż nastąpiłoby to na podstawie zgłoszeń abonentów do CSIRT NASK, jak proponuje się w art. 4 ust. 1 projektu.  Stanowczo ponownej analizy pod kątem jej proporcjonalności i celowości wymaga procedura opisana w art. 4. W szczególności:  - w ust. 1 celowym byłoby rozszerzenie zakresu nadużyć, które mogą być zgłaszane CSIRT NASK także do innych nadużyć w komunikacji elektronicznej, których przedmiotem jest komunikacja SMSowa;  - w ust. 2 dostęp do wykazu wzorców SMS zawierających smishing powinien mieć nie tylko przedsiębiorca telekomunikacyjny, ale też integrator SMS, który mógłby usuwać smishing zanim trafi on do sieci telekomunikacyjnej. Dzięki temu podmiot ten mógłby również korygować zlecane mu SMS A2P od jego klientów, jeśli byłyby one zbieżne z wzorami z wykazu CSIRT NASK;  - w ust. 3 niejasne jest jakie informacje o wystąpieniu smishingu CSIRT NASK miałby przekazywać przedsiębiorcom telekomunikacyjnym, wraz ze wzorcem wiadomości wyczerpującej znamiona smishingu i jaki byłby cel tak szerokiego informowania o wystąpieniu smishingu np. w odniesieniu do poszczególnych numerów wraz z danymi abonentów potencjalnie stanowiącymi przedmiot tajemnicy telekomunikacyjnej;  - w ust. 3 niezrozumiała jest też koncepcja „wzorca” wiadomości, w szczególności czy obejmuje ona także konkretny link, który prowadził do stron służących do nadużyć. W przypadku, w którym taka informacja nie byłaby zawarta we wzorcu KIKE zwraca uwagę, że w niektórych wypadkach określenie takiego wzorca może skutkować zablokowaniem ruchu niemającego na celu popełniania nadużyć (np. standardowa informacja o paczce oczekującej na odbiór czy SMS o treści odpowiadającej autoryzacji może, ale nie musi być wykorzystywana do nadużyć). Wprowadzenie ogólnego zakazu stosowania takiego wzorca doprowadziłoby do zablokowania komunikacji o takiej treści, mogąc stanowić wręcz potencjalny i samodzielny przedmiot ataków zmierzających do ograniczenia niektórych form komunikacji;  - w ust. 3 analizy pod kątem obciążenia pracy policji wymaga, czy każda informacja o wystąpieniu smishingu faktycznie winna być przekazywana Komendantowi Głównemu Policji;  - w ust. 4 zaproponowany termin 14-21 dni na publikację w wykazie nowego wzorca jest okresem nie tylko niezrozumiałym (nie wiadomo która z tych dat jest właściwa i w jakiej sytuacji), ale i stanowczo zbyt długim dla tego rodzaju nadużyć. W opinii Izby publikacja stwierdzonego smishingu jako nowego wzorca powinna nastąpić w terminie maksymalnie pół godziny od jego doręczenia CSIRT NASK;  - w ust. 5-6 niezrozumiałe są konsekwencje uznania co do treści zawartej we wzorcu – czy w takim wypadku dalszemu blokowaniu nie podlega wzorzec, czy konkretna wiadomość, która miała stanowić przedmiot smishingu?  - w art. 5 ust. 1 dochodzi do zmiany pojęcia „wzorca” na treść, co wpływa na brak jasności przepisu, w szczególności wobec braku wskazania podmiotu, który miał uznać tę treść za wyczerpującą znamiona smishingu,  - w art. 5 ust. 2 sprzeciw zawierać ma m.in. wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej, którego Prezes UKE nie zna – z CSIRT NASK otrzymuje bowiem wyłącznie treść wzorca. Cel wskazania tego numeru jest więc nieznany,  - w art. 6 ust. 1 pkt 1 nie została określona forma rozpatrzenia sprzeciwu, w szczególności nie zostały poddane analizie konsekwencje związane z obciążeniem Prezesa UKE oraz sądów pracą związaną z rozpatrywaniem sprzeciwów w formie decyzji. Jest też więcej niż racjonalnym, by działanie to było poprzedzone wezwaniem właściwego przedsiębiorcy telekomunikacyjnego. Niejasna jest także relacja tej procedury do procedury reklamacji,  - w art. 6 ust. 2, w wyniku uwzględnienia sprzeciwu Prezes UKE przekazuje wybranym podmiotom informację, że „treść zawarta we wzorcu wiadomości nie stanowi smishingu”. Informacja ta pozostaje niespójna z przedmiotem postępowania w sprawie sprzeciwu, którego istotą zdaje się być rozpatrzenie przypadku blokady konkretnego SMSa. | **Uwaga częściowo uwzględniona** w zakresie otworzenia katalogu podmiotów, które sygnalizują CSIRT NASK wystąpienie smishingu  **Uwaga nieuwzględniona w pozostałym zakresie**  Opisany mechanizm dotyczy publikacji wzorca dla wszystkich odbiorców, a nie jego przekazania do przedsiębiorców telekomunikacyjnych. Przekazanie wzorca do przedsiębiorcy następuje niezwłocznie po jego wytworzeniu przez CSIRT NASK.  W związku z tym ochrona konsumentów będzie następować w najszybszym możliwym terminie. Dopiero później wzorzec będzie dostępny publicznie.  Upublicznienie wzorca równocześnie z przesłaniem go do przedsiębiorców telekomunikacyjnych mogłoby pozwolić sprawcom przestępstw natychmiast zmienić stosowane przez nich wiadomości, co przełożyłby się na zniwelowanie skuteczności projektowanego rozwiązania i tym samym godziłoby w realizację celu ustawy.  W zakresie stosowania wzorca należy zauważyć, że opracowana została procedura sprzeciwu w ramach, której użytkownik będzie mógł zgłosić sprzeciw gdy jego wiadomości zostaną zablokowane jako wpisujące się w zorze. W przypadku gdy Prezes UKE uzna sprzeciw za zasadny CSIRT NASK będzie obowiązany do jego zmiany. Ta procedura będzie chroniła prawa użytkowników oraz pozwoli CSIRT NASK udoskonalać wykorzystywane wzorce.  To jakie informacje będzie przesyłał CSIRT NASK wraz ze wzorem będzie oceniane indywidualnie w poszczególnych przypadkach. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 4 ust. 1 | **Monitorowanie smishingu przez CSIRT NASK** (art. 4 ust. 1 projektu ustawy)  Projekt ustawy stanowi, że CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu. Nie ulega wątpliwości, że przynajmniej część sygnałów o nadużyciach NASK będzie otrzymywał do odbiorców wiadomości SMS. Niemniej jednak zasadnym wydaje się założenie, że NASK może otrzymywać sygnały o kampaniach smishingowych nie tylko od odbiorców tych wiadomości, ale również od organów ścigania, regulatora rynku telekomunikacyjnego, podmiotów zajmujących się bezpieczeństwem, instytucji publicznych i przedsiębiorców prywatnych. A skoro tak, to nieuzasadnione jest ustawowe ograniczanie CSIRT NASK tylko do jednego źródła informacji, gdyż takie rozwiązane w sposób nieuzasadniony ograniczy skuteczność działania CSIRT NASK, który powinien móc korzystać z każdego legalnego źródła informacji do identyfikowania kampanii smishingowych.  W związku z powyższym zasadnym wydaje się nadanie art. 4 ust. 1 projektu ustawy następującego brzmienia:  *CSIRT NASK ~~na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS)~~ monitoruje występowanie smishingu.*  Alternatywnie, analizowany przepisów mógłby uzyskać następujące brzmienie:  *CSIRT NASK, w szczególności na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS), monitoruje występowanie smishingu.* | **Uwaga uwzględniona** **w zakresie otwarcia katalogu podmiotów, które mogą przesyłać sygnały do CSIRT NASK** |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 4 ust. 1 i ust. 2 | **Art. 4 ust. 1 i ust. 2**  Realizacja przedsięwzięć określonych w art. 4 projektu będzie związana z bardzo poważną ingerencją w prywatność wszystkich osób przesyłających krótkie wiadomości tekstowe (SMS), nie tylko tych, wobec których podejmowane będą próby smishingu.  Odbiorcy SMS (co najmniej dwóch – tylko dwóch) zainicjuje monitorowanie przez CSIRT NASK występowanie smishingu.  Na podstawie takiego monitorowania (może lepiej będzie brzmiało: po analizie wyników monitorowania) CSIRT NASK tworzy wzorzec wiadomości.  W projekcie nie wskazano podmiotów (organów) oraz narzędzi weryfikujących poprawność opracowanego przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu.  Jedynymi przesłankami umożliwiającymi uznanie wiadomości SMS jako smishing są te, które zostały zawarte w definicji smishingu (art. 3 ust. 1 pkt 2 projektu).  Wobec bardzo ogólnych przesłanek, na podstawie których kwalifikuje się zdarzenie jako nadużycie w komunikacji elektronicznej CSIRT NASK otrzymuje ustawowe prawo dużej swobody w tworzeniu wzorca wiadomości wyczerpującej znamiona smishingu.  **Należałoby zatem postulować wskazanie w projekcie niezależnego podmiotu lub organu uprawnionego do zatwierdzania stworzonego przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu, którego decyzja dopiero pozwalałaby na opublikowanie przedmiotowego wzorca wiadomości wyczerpującej znamiona smishingu w sposób określony w art. 4 ust. 4 projektu, względnie stanowiłaby przeciwwskazanie do dokonania tego rodzaju publikacji obligując zarazem CSIRT NASK do poprawy, czy też przeróbki wzorca wiadomości wyczerpującej znamiona smishingu.**  Jest to o tyle istotne, gdyż rzeczywiste zwalczanie smishingu, w sposób określony w projekcie będzie realizowane przez przedsiębiorcę telekomunikacyjnego kierującego się wzorcem wiadomości wyczerpującej znamiona smishingu opracowanym przez CSIRT NASK (art. 4 ust. 6 pkt. 1 projektu), a zupełnie wyjątkowo wedle subiektywnego przekonania przedsiębiorcy telekomunikacyjnego dokonywanego w oderwaniu od przedmiotowego wzorca (art. 7 projektu). | **Uwaga wyjaśniona**  Monitorowanie przez CSIRT NASK występowania smishingu oraz tworzenie wzorców wiadomości smishingowych ma charakter czynności technicznych. Poprzez procedurę sprzeciwu zapewnia się możliwość zmiany wzorca wiadomości. W projekcie została przewidziana procedura w ramach, której wzorzec będzie ulepszany. Zapewni to nie tylko ochronę praw użytkowników, ale pozwoli ulepszyć wzorzec tak aby lepiej pełnił swoją rolę. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 4 ust. 4 | **Publikowanie wzorców smishingowych**  Projektowany art. 4 ust. 4 zakłada, że CSIRT NASK będzie publikował na swojej stronie internetowej wzorce wiadomości smishingowych. W naszej ocenie przepis ten powinien zostać usunięty z projektu ustawy, gdyż wzorce nie powinny być publikowane ze względów bezpieczeństwa. Opublikowane wzorce mogą stanowić dla przestępców wskazówki zarówno co do metodologii działania CSIRT NASK jak i sposobu blokowania takich wiadomości przez przedsiębiorców telekomunikacyjnych, co może służyć do opracowywania metod obchodzenia stosowanych rozwiązań anty-smishingowych. | **Uwaga nieuwzględniona**  Jawność wzorca wiadomości smishingowej jest niezbędna dla zapewnienia przejrzystości procesu blokowania wiadomości a także jest niezbędne dla zagwarantowania praw użytkowników i możliwości skorzystania z instytucji sprzeciwu przez nadawcę wiadomości, która została zablokowana jako wpisująca się we wzorzec. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 4 ust. 4 | **Art. 4 ust. 4**  Przedmiotowa regulacja wymaga dokonania precyzyjnej korektury.  O ile określenie terminu końcowego udostępnienia przez CSIRT NASK wzorca wiadomości wyczerpującej znamiona smishingu nie nastręcza nadmiernych trudności (21 dni od dnia przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w ust. 3), to już określenie początkowego terminu publikacji tegoż wzorca w rzeczywistości jest zawieszone w prawnej próżni.  W sytuacji gdy projektodawca podaje, że wzorzec zostaje udostępniony na stronie internetowej CSIRT NASK w terminie 14 dni, nie później jednakże niż 21 dni od dnia przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w ust. 3 termin początkowy winien być do czegoś odniesiony.  Tymczasem w proponowanej regulacji nie wiemy w odniesieniu do jakiegoż momentu w czasoprzestrzeni należy odnieść ten termin 14- dniowy, czy termin ten liczony jest od dnia stworzenia przez CSIRT NASK przedmiotowego wzorca(akurat tak określony moment byłby trudny do zweryfikowania), czy też liczony jest od przekazania wzorca przedsiębiorcy telekomunikacyjnemu w sposób określony w art. 4 ust. 3 projektu.  Od razu należy wskazać, że w przedmiotowym przepisie tak naprawdę jedynym istotnym terminem jest termin końcowy publikacji wzorca, bo ten termin początkowy w tego rodzaju regulacji prawnej pozbawiony jest jakiegokolwiek znaczenia, skoro istotne jest by ten wzorzec opublikować w terminie 21 dni od dnia udostepnienia przedsiębiorcy w sposób opisany w art. 4 ust. 3 projektu.  Inna sprawa to ta, że przedmiotowa norma pozbawiona jest jakiegokolwiek „ostrza”, bo co się stanie jeśli CSIRT NASK nie zachowa terminu ustawowego opublikowania na swojej stornie internetowej przedmiotowego wzorca.  Czy w takim przypadku np. publikując wzorzec przed 14 dniem liczonym od nie wiadomo jakiego momentu, czy też po upływie 21 dnia od przekazania przedsiębiorcy telekomunikacyjnemu tegoż wzorca w sposób określony w art. 4 ust. 3 projektu wzorzec nie nabędzie mocy obowiązującej i nie będzie wywoływał skutków prawnych związanych z jego opublikowaniem, a zatem nie będzie mógł stanowić podstawy do blokowania SMS-ów, czy tez uchybienie temu terminowi wywoła inne skutki prawne, których projektodawca nam niestety nie ujawnia.  W takim przypadku możnaby wprowadzić regulację przewidującą, iż w razie uchybieniu terminowi publikacji wzorca CSIRT NASK byłby zobowiązany do zapłaty kary administracyjnej w wysokości 1 mln zł na Fundusz Cyberbezpieczeństwa.  W tym miejscu z przykrością należy stwierdzić, że projektodawca przewidując kary administracyjne o charakterze pieniężnym w art. 15 i art. 16 projektu nie przewiduje kary nakładanej na CSIRT NASK w razie uchybienia terminowi opublikowania wzorca wiadomości wyczerpującej znamiona smishingu, przewidując jedynie kary nakładane na przedsiębiorców telekomunikacyjnych.  **Podsumowując tę część rozważań na okoliczność niewskazania w projekcie jakichkolwiek skutków prawnych związanych z uchybieniem przez CSIRT NASK terminowi opublikowania wzorca wiadomości wyczerpującej znamiona smishingu proponujemy w art. 4 ust. 4 projektu ograniczyć regulację jedynie do wskazania, że przedmiotowy wzorzec CSIRT NASK opublikuje na swojej stronie internetowej bez określania terminu początkowego oraz końcowego dokonania publikacji albowiem w proponowanej wersji przepisu terminy te pozbawione są jakiegokolwiek znaczenia prawnego.**  **Jeżeli natomiast w projekcie projektodawca zdecyduje się na wprowadzenie regulacji przewidującej lub przewidujących skutki prawne powiązane z zachowaniem przez CSIRT NASK terminu publikacji przedmiotowego wzorca, wówczas proponujemy usunięcie terminu początkowego przewidzianego w art. 4 ust. 4 projektu, a pozostawienie wyłącznie terminu końcowego, do którego przedmiotowy wzorzec winien zostać opublikowany albowiem w proponowanej obecnie regulacji ten termin początkowy, w dodatku liczony od bliżej nieokreślonego momentu w czasoprzestrzeni, nie odgrywa jakiejkolwiek prawem określonej roli.** | **Uwaga częściowo uwzględniona**  Przepis zostanie doprecyzowany aby jasno wskazywał, że CSIRT NASK publikuje wzorzec nie wcześniej niż po 14 dniach (i nie później niż 21 dni) od przekazania wzorca za pomocą systemu teleinformatycznego. |
|  | Związek Banków Polskich | **Art. 4 ust. 6 pkt 3** | **3) poinformowania podmiotu, pod który podszywa się nadawca wiadomości, o której mowa w ust. 3. W przypadku podszycia się pod podmiot, o którym mowa w art. 106d ust. 1 lub 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.) przedsiębiorca telekomunikacyjny jest zobowiązany do poinformowania centrum wymiany i analizy informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.);**  Kluczowe dla przeciwdziałania skutkom nadużycia w komunikacji elektronicznej jest niezwłoczne poinformowanie o fakcie smishingu lub spoofingu podmiotu, pod który podszywają się przestępcy. Tego rodzaju działanie pozwala na odpowiednio wczesne ostrzeżenie klientów (w przypadku przedsiębiorcy), co jest szczególnie istotne w przypadku klientów sektora finansowego. Banki oraz FinCERT.pl – BCC ZBP niezwłocznie po zidentyfikowaniu takich zagrożeń opracowują ostrzeżenia, które są propagowane używanymi kanałami komunikacji z klientami. Przekazanie tych informacji do centrum wymiany i analizy informacji dla sektora finansowego – FinCERT.pl – BCC ZBP ma istotne znaczenie w kontekście poinformowania innych instytucji o prowadzonych kampaniach przestępczych. | **Uwaga nieuwzględniona**  w związku z nieuwzględnieniem uwagi o zmianach w Prawie bankowym. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | **Art. 4 ust. 6 pkt 1, art. 7** | Proponowana wersja przedmiotowego przepisu razi małą precyzyjnością z czym nie możemy mieć do czynienia w przypadku przepisów, które wdrażane są w celach zapewnienia bezpieczeństwa w komunikacji elektronicznej.  Określenie bowiem zawarte w tym przepisie nakładające na przedsiębiorcę telekomunikacyjnego obowiązek „niezwłocznego” blokowania SMS-ów zawierających treści zawarte we wzorcu prowadzi do stosowania pojęcia niedookreślonego, stanowiącego autostradę wręcz do różnorakich interpretacji.  W sprawach cywilnych wedle ukształtowanych od lat w orzecznictwie sadowym zapatrywań niezwłoczność podjęcia jakiegoś działania określano na termin 14- dniowy.  W przypadku czynów zabronionych w telekomunikacji określonych w art. 3 ust. 1 pkt. 2 projektu termin 14- dniowy na zablokowanie SMS-a wyczerpującego znamiona smishingu określone we wzorcu wydaje się terminem zbyt długim i trudnym do wdrożenia w praktyce.  Aby prawidłowo zastosować przedmiotowy przepis oznaczałoby to, że przedsiębiorca telekomunikacyjny przez okres nie dłuższy niż 14 dni uprawniony by był przetrzymywać wszystkie wysłane w jego sieci SMS-y, aby w tym okresie sprawdzić, czy nie spełniają one znamion smishingu określonych we wzorcu i jeśli nie spełniają to przed upływem 14 dnia od jego zatrzymania musiałby go puścić dalej, a jeśli spełniają wówczas byłby obowiązany z nastaniem 14 dnia od zatrzymania SMS- a dokonać jego zablokowania.  Regulacja taka wydaje się wręcz absurdalna, zaś zatrzymywanie wszystkich SMS-ów wysłanych w sieci telekomunikacyjnego danego operatora przez okres nie dłuższy niż 13 dni jeśli nie spełniają znamion smishingu oraz ich blokowanie z 14 dniem od ich zatrzymania w przypadku, gdy spełniają znamiona smishingu w zasadzie przeczy instytucji krótkiej wiadomości tekstowej albowiem żaden abonent nie będzie zainteresowany korzystaniem z usługi odnośnie której będzie wiedział, że wysłana wiadomość do adresata może dotrzeć np. w 13 dniu od wysłania i wszystko w takim przypadku będzie znajdowało oparcie w obowiązującym prawie.  Takie rozwiązanie jest wręcz niebezpieczne albowiem możemy sobie wyobrazić sytuację, że turysta spada zimą w przepaść i łamie nogę i wysyła do TOPR-u lub GOPR-u sms- a z prośbą o pomoc lub ratunek, który przez 13 dni jest przetrzymywany przez przedsiębiorcę telekomunikacyjnego celem przeanalizowania czy rzeczona wiadomość nie spełnia znamion smishingu i dopiero z 13 dniem zgodnie z prawem przedsiębiorca telekomunikacyjny puszcza tego sms-a do TOPR-u lub GOPR-u.  W takiej sytuacji niewątpliwie ratownicy górscy winni ze sobą wziąć jedynie worek na zwłoki, bo sprzęt medyczny nie będzie już do niczego przydatny.  **W projekcie i to tak w art. 4 ust. 6 pkt. 2 w odniesieniu do dokonania przez przedsiębiorcę telekomunikacyjnego oceny czy SMS spełnia znamiona smishingu określone we wzorcu, jak i w art. 7 w odniesieniu do dokonania przez przedsiębiorcę telekomunikacyjnego oceny czy SMS spełnia znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu nieujęte we wzorcu opublikowanym przez CSIRT NASK na stronie internetowej CSIRT NASK należy określić maksymalny, stosunkowo krótki okres czasu liczony w minutach, w którym przedsiębiorca może dokonać oceny, a na jej podstawie dokonać decyzji o zablokowaniu SMS- a lub też o jego puszczeniu dalej do adresata.** | **Uwaga wyjaśniona**  W przypadku tej regulacji nie należy wykładać pojęcia „niezwłoczności” jako 14 dni tak jak jest to wyrażone w niektórych liniach orzeczniczych sądów powszechnych do art. 455 Kodeksu cywilnego. Mamy tutaj do czynienia z przepisami prawa administracyjnego, a nie prawa prywatnego.  Zostanie wyjaśnione w uzasadnieniu, że niezwłoczność należy rozumieć w ten sposób, że przedsiębiorca telekomunikacyjny będzie obowiązany zablokować wiadomości smishingowe najszybciej jak będzie mógł, a więc z zachowaniem zasady *impossibilium nulla obligatio est*.  Wskazać również należy, że opóźnienie blokowania wiadomości smishingowych może spowodować straty wizerunkowe po stronie przedsiębiorcy telekomunikacyjnego, ponieważ mimo tego, że wiedział o złośliwych wiadomościach to zezwolił na ich przesłanie co naraża jego klientów na ryzyko strat. |
|  | IAB Polska | Art. 5, Art. 6 | **UWAGA:**  W Art. 5 UZNKE zostało uregulowane prawo nadawcy krótkiej wiadomości tekstowej (SMS) do wniesienia sprzeciwu do Prezesa UKE wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu. Z przepisów UZNKE **nie wynika, w jakim trybie jest rozpatrywany sprzeciw Prezesa UKE**, m.in. przy uwzględnieniu przepisów jakiej procedury powinna być badana przez Prezesa UKE zasadność sprzeciwu złożonego przez nadawcę SMS, jaką formę prawną przybiera rozstrzygnięcie Prezesa UKE uwzględniające lub nieuwzględniające sprzeciwu lub czy nadawca, który nie jest zadowolony z rozstrzygnięcia Prezesa UKE, mam możliwość zakwestionowania zasadności i legalności takiej decyzji, dzięki instancji odwoławczej.  **PROPOZYCJA:**  Projektodawca powinien doprecyzować tę kwestię, m.in. określić, czy Prezes UKE powinien stosować przepisy postępowania administracyjnego przy podejmowaniu decyzji o uwzględnieniu sprzeciwu, jaką formę prawną powinny przyjąć rozstrzygnięcia podejmowane w tej kwestii przez Prezesa UKE i czy istnieje możliwość badania zasadności i legalności tych rozstrzygnięć. | **Wyjaśnienie**  Rozpatrzenie sprzeciwu nie następuje w drodze decyzji administracyjnej i nie wymaga zachowania szczególnej formy. Jest to w ocenie projektodawcy tzw. inna czynność z zakresu administracji publicznej, która podlega kontroli sądu administracyjnego. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 5 | **ad Art. 5. ust. 1.** Nadawca krótkiej wiadomości tekstowej (SMS) może wnieść do Prezesa UKE sprzeciw wobec uznania treści takiej wiadomości za wyczerpującą znamiona smishingu.  **ust. 2.** Sprzeciw zawiera: 1) uzasadnienie wyjaśniające dlaczego treść krótkiej wiadomości tekstowej (SMS) nie wyczerpuje znamion smishingu;  Komentarz PTI  W przypadku zaakceptowania propozycji PTI powyżej do art. 4 ust. 2 powyższy przepis nie budzi wątpliwości. Jednakże pozostawienie takiej treści art. 5.1 i 2 bez proponowanej zmiany PTI w art. 4 ust. 2 spowoduje, iż nie będzie możliwe skuteczne sprzeciwienie się zarzutowi szalbierstwa w esemesie (smishingu), ponieważ nie będą jawne wskazane (nie będą ogłoszone) zarzuty uzasadniające blokadę. Byłoby to sprzeczne z jedną spośród zasad prawodawstwa, iż wymagane może być tylko prawo ogłoszone. | **Uwaga wyjaśniona**  Przepisy ustawy wyraźnie wskazują, że użytkownicy będą mogli zgłaszać sprzeciw do Prezesa UKE i przez to wskazywać, że wzorzec przygotowany przez NASK jest niedoskonały. W przypadku gdy prezes UKE uwzględni sprzeciw, CSIRT NASK będzie musiał zmienić swój wzorzec. Będzie to skuteczny sposób podważania wzorca smishingu. Ponadto, zmiana wzorca będzie mogła nastąpić w trybie autokontroli przez CISRT NASK (przedsiębiorcy telekomunikacyjnemu w sposób, o którym mowa w ust. 3.  6. CSIRT NASK, w przypadku gdy uzna, że:  1) treść zawarta we wzorcu wiadomości nie stanowi smishingu, lub  2) niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS) zgodnych ze wzorcem wiadomości niezwłocznie  - informuje o tym podmioty, o których mowa w ust. 3 oraz zamieszcza na stronie internetowej informacje o okresie w jakim wzorzec obowiązywał). |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 5 ust. 1 | **Art. 5 ust. 1**  Przedmiotowa regulacja budzi uzasadnioną wątpliwość natury prawnej.  Projektodawca uznał, że sprzeciw winien być wnoszony od uznania treści krótkiej wiadomości tekstowej za wyczerpującą znamiona smishingu, gdy tymczasem rzeczywistym powodem jego wniesienia przez nadawcę SMS- a jest zablokowanie krótkiej wiadomości tekstowej przez przedsiębiorcę telekomunikacyjnego, a nie powody dokonania blokady (art. 4 ust. 6 pkt. 1 projektu, art. 7 projektu).  Mało tego, można sobie przecież wyobrazić sytuację, że przedsiębiorca telekomunikacyjny, mimo iż uznał, że krótka wiadomość tekstowa spełnia znamiona smishingu, a jednak nie zdecydował się na jej zablokowanie.  O ile sytuacja taka zupełnie wyjątkowo może zaistnieć w przypadku SMS- a spełniającego znamiona smishingu określone we wzorcu takiej wiadomości, gdyż w takim przypadku przedsiębiorca telekomunikacyjny zobowiązany jest do zablokowania takiej wiadomości (art. 4 ust. 6 pkt. 1 projektu), to już w przypadku krótkiej wiadomości tekstowej spełniającej znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu nie objęte jednakże wzorcem opublikowanym na stronie internetowej CSIRT NASK taka sytuacja może wręcz stanowić prawidłowość, gdyż wolą projektodawcy w takim przypadku od woli przedsiębiorcy telekomunikacyjnego zależy czy taką wiadomość zablokuje, czy też nie, skoro projektodawca na taką okoliczność przyznał przedsiębiorcy telekomunikacyjnemu prawo, a nie obowiązek(jak w art. 4 ust. 6 pkt. 1 projektu) blokowania takich wiadomości (art. 7 projektu).  Jeżeli zatem krótka wiadomość tekstowa zostanie uznana za spełniającą znamiona smishingu, ale przez przedsiębiorcę telekomunikacyjnego nie zostanie zablokowana, to w takim przypadku zupełnie bezprzedmiotowe staje się przyznanie nadawcy SMS-a uprawnienia do wniesienia sprzeciwu, skoro SMS nie został zablokowany.  Mało tego, w takim przypadku regulacja art. 5 ust. 1 projektu przyznająca nadawcy SMS-a prawo do wniesienia sprzeciwu do Prezesa UKE, mimo niezablokowania SMS- a spełniającego znamiona smishingu kłóci się z pojęciem strony uregulowanym w art. 28 k.p.a. albowiem trudno byłoby przyznać w postępowaniu administracyjnym status strony nadawcy SMS-a, który nie został zablokowany, mimo spełnienia znamion smishingu, gdyż tenże nadawca nie posiadałby żadnego interesu prawnego w zaskarżeniu uznania krótkiej wiadomości tekstowej za spełniającą znamiona smishingu, w sytuacji, gdyby przedsiębiorca telekomunikacyjny nie zablokował tegoż SMS-a.  Regulację art. 5 ust. 1 projektu uznać należy za wadliwą jeszcze z jednego powodu, a mianowicie z uwagi na jej nieracjonalność.  W jakiej bowiem sytuacji zdaniem projektodawcy dojdzie do powzięcia przez nadawcę krótkiej wiadomości tekstowej wiedzy o tym, iż przedsiębiorca telekomunikacyjny uznał nadanego SMS-a za wyczerpujący znamiona smishingu, skoro nie doszło do zablokowania jego wysyłki.  Nie posiadając zaś wiedzy o uznaniu SMS-a za spełniający wymogi smishingu wobec jego niezablokowania nadawca tejże wiadomości nie mógłby wnieść sprzeciwu, skoro nie wiedziałby o dokonaniu takiej oceny przez przedsiębiorcę telekomunikacyjnego.  **W kwestionowanej zatem regulacji przedmiotem sprzeciwu wnoszonego do Prezesa UKE nie powinno być uznanie treści SMS-a za wyczerpującą znamiona smishingu, ale zablokowanie przez przedsiębiorcę telekomunikacyjnego krótkiej wiadomości tekstowej z powodu uznania rzeczonej wiadomości przez przedsiębiorcę telekomunikacyjnego za spełniającą znamiona smishingu**. | **Uwaga wyjaśniona**  Nadawca będzie mógł zgłosić sprzeciw od zablokowania sms wobec zablokowania krótkiej wiadomości tekstowej (SMS) zawierającej treści zawarte we wzorcu wiadomości.  W zakresie stosowania wzorca należy zauważyć, że opracowana została procedura sprzeciwu w ramach, której użytkownik będzie mógł zgłosić sprzeciw gdy jego wiadomości zostaną zablokowane. W przypadku gdy Prezes UKE uzna sprzeciw za zasadny CSIRT NASK będzie obowiązany do jego zmiany. Ta procedura będzie chroniła prawa nadawcy oraz pozwoli CSIRT NASK udoskonalać wykorzystywane wzorce.  Sprzeciw nie będzie przysługiwał od zablokowania wiadomości przez przedsiębiorcę telekomunikacyjnego w związku z uzupełniającym uprawnieniem (art. 7 projektu). W przypadku zablokowania na tej podstawie użytkownik końcowy będzie mógł skorzystać m.in. z reklamacji.  Do instytucji sprzeciwu nie będą stosowane przepisy KPA. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 5 ust. 2 pkt 2 | **VI. [TREŚĆ SPRZECIWU – ART. 5 UST. 2 PKT 2)]**  **(27.)** W tym zakresie wskazano, że wymaganiem koniecznym (brakiem formalnych) jest „*wskazanie numeru wykorzystanego do nadania krótkiej wiadomości tekstowej (SMS)*”.  **(28.)** Zwracamy uwagę, że często wiadomość SMS może nie być identyfikowana przez numer, ale nazwę. Na przykład alerty są opisywane nie numerem ale nazwą (np. „ALERT RCB”).  **(29.)** W konsekwencji jak się wydaje ten element sprzeciwu powinien brzmieć „*wskazanie numeru lub nazwy wykorzystanej do nadania krótkiej wiadomości tekstowej (SMS)*”. | **Uwaga nieuwzględniona**  Obecne regulacje dotyczące sprzeciwu są uregulowane w taki sposób aby umożliwić skuteczne wniesienie sprzeciwu. Sprzeciw dotyczy wiadomości, która została zablokowana ze względu na wpisanie się we wzorzec wiadomości wyczerpującej znamiona smishingu, a więc będzie zgłaszany przez wysyłającego wiadomość. Wysyłający zna numer, który wykorzystywał a więc nie dojdzie do sytuacji w której zgłaszający sprzeciw nie będzie znał wykorzystywanego numeru. Nie jest więc konieczne wprowadzanie proponowanej zmiany. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 5 ust. 3 | **Art. 5 ust. 3**  Zdecydowanie należy sprzeciwić się wymogowi opatrywania sprzeciwu podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym i wnoszeniu tegoż sprzeciwu za pomocą środków komunikacji elektronicznej.  Wyobraźmy sobie 100- letniego pana, który jako tako radzi sobie z komórką i mieszka w Bieszczadach lub innych wysokich górach, gdzie dostęp do Internetu jest iluzoryczny, czy wręcz żaden.  Czy autorzy projektu oczekują, że ten 100- letni starszy pan posiada wyrobiony jakikolwiek podpis elektroniczny którego brak pozbawia jego osobę możliwości wniesienia sprzeciwu przeciwko uznania treści jego krótkiej wiadomości tekstowej nadanej do wnuczki za spełniającą znamiona smishingu.  Co więcej, projektodawca oczekuje od tego 100- letniego starszego pana umiejętności korzystania ze środków komunikacji elektronicznej, bo tylko tą drogą można wnieść sprzeciw do Prezesa UKE.  Mało tego, gdyby nawet ten 100- letni starszy pan zamieszkujący w wysokich górach jakimś cudem zadbał o posiadanie jakiegokolwiek podpisu elektronicznego i w dodatku posiadł umiejętność korzystania ze środków komunikacji elektronicznej (chyba wszyscy czujemy, że są to założenia mało prawdopodobne do zaistnienia), to w sytuacji gdy zamieszkuje w tych wysokich górach będąc osobą mocno schorowaną nie ma żadnych szans wysłania sprzeciwu przy wykorzystaniu środków komunikacji elektronicznej, gdyż środki te w tamtym terenie po prostu nie działają z uwagi na brak dostępu do Internetu, a trudno oczekiwać, by ten pan mieszkając w 200- letniej drewnianej chałupie posiadał tam dostęp do Internetu satelitarnego.  Należy zważyć, że Prezes UKE rozpoznając sprzeciw wydaje decyzję administracyjną (art. 104 1 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego).  Ponieważ decyzja w przedmiocie rozpoznania sprzeciwu nie należy do grupy decyzji wymienionych w art. 206 ust. 2 prawa telekomunikacyjnego, przeto od decyzji w przedmiocie rozpoznania sprzeciwu nie wnosi się odwołania do Sądu Ochrony Konkurencji i Konsumentów lecz zaskarżając ją składa się wniosek o ponowne rozpoznanie sprawy przez Prezesa UKE (art. 127 § 3 k.p.a. w zw. z art. 5 § 2 pkt. 4 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego).  Oznacza to, iż od decyzji wydanej przez Prezesa UKE w przedmiocie rozpatrzenia wniosku o ponowne rozpatrzenie sprawy zaskarżającego decyzję w przedmiocie rozpoznania sprzeciwu strona postępowania może zaskarżyć do Wojewódzkiego Sądu Administracyjnego w Warszawie stosowną skargą[ art. 3 § 2 pkt. 1 ustawy z dnia 30.08.2002 r. prawo o postepowaniu przed sądami administracyjnymi (tekst jedn .Dz. U. z 2022 r. poz. 329 z późn. zm.), zwanej dalej p.p.s.a.].  W przedstawionym przez nas stanie faktycznym, a przecież porównywalnych stanów faktycznych może być o wiele więcej, projektodawca art. 5 ust. 3 pozbawia obywatela będącego nadawcą krótkiej wiadomości tekstowej konstytucyjnie mu przysługującego prawa do sądu albowiem skoro nie wniesie on sprzeciwu, bo nie posiada jakiegokolwiek podpisu elektronicznego, osobistego lub zaufanego lub nie włada środkami komunikacji elektronicznej, czy też przedmiotowe środki nie mogą być w jego sytuacji życiowej wykorzystane, a najczęściej wszystkie te trzy ograniczenia wystąpią łącznie, jak w podanym przez nas przykładzie.  Regulacja zatem art. 5 ust. 3 projektu jako pozbawiająca potencjalną stronę postępowania administracyjnego przysługującego jej konstytucyjnego prawa do sądu przewidzianego w art. 45 ust. 1 w zw. z art. 77 ust. 2 Konstytucji Rzeczypospolitej Polskiej z dnia 2.04.1997 r. (Dz. U. nr 78 poz. 483 z późn. zm.), zwanej dalej Konstytucją RP, a zatem łamiąca najwyższe prawo obowiązujące w naszym kraju znajdujące bezpośrednie zastosowanie w wewnętrznym porządku prawnym (art. 8 Konstytucji RP), jako norma niekonstytucyjna ostać się nie może.  Wniesienie zatem sprzeciwu winno być przez projektodawcę dopuszczone w każdej formie prawnej dopuszczonej przez przepisy k.p.a., w tym i w formie pisemnej.  **W zaistniałej sytuacji proponujemy zatem skreślenie regulacji art. 5 ust. 3 projektu** albowiem formy prawne wniesienia sprzeciwu będą wówczas regulowane przez przepisy k.p.a. | **Uwaga nieuwzględniona**  Uprawnionym do wniesienia sprzeciwu jest nadawca wiadomości, która została zablokowana w zw. z zastosowaniem wzorca wiadomości wyczerpującej znamiona smishingu. Sprzeciw opatruje się kwalifikowanym podpisem elektronicznym, podpisem zaufanym albo podpisem osobistym.  Profil zaufany to bezpłatna metoda potwierdzania tożsamości obywatela w systemach podmiotów publicznych. Można za jego pomocą zalogować się do takiego systemu, a w razie takiej potrzeby złożyć podpis elektroniczny (podpis zaufany), który wobec podmiotów publicznych jest równie skuteczny jak podpis własnoręczny.  Podpis osobisty to zaawansowany podpis elektroniczny związany z e-dowodem (dowodem osobistym z warstwą elektroniczną). Prawdziwość danych posiadacza podpisu potwierdza certyfikat podpisu osobistego, zawierający imię (imiona), nazwisko, obywatelstwo oraz numer PESEL.  Aby certyfikat podpisu osobistego znalazł się w e‑dowodzie, należy wyrazić na to zgodę podczas składania wniosku o nowy dokument.  Wprowadzenie takiego rozwiązania dla którego komunikacja z urzędem odbywa się drogą elektroniczną jest rozwiązaniem proporcjonalnym i adekwatnym. Pozwala jednoznacznie i w prosty sposób zidentyfikować personalia osoby wnoszącej sprzeciw, co zmniejszy możliwość obstrukcji organu oraz możliwość podważania wzorców przez osoby, które podszywałyby się pod nadawcę, oraz zapewni prawne procesowanie tego specyficznego postępowania. Przedmiotem tego postępowania jest zmiana wzorca ze skutkiem dla wszystkich uczestników obrotu, a nie jedynie realizowanie indywidualnych uprawnień, które są zapewnione innymi instytucjami prawnymi. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 6 | **VII. [FORMA PRAWNA ROZPATRZENIA SPRZECIWU]**  **(30.)** Projekt nie wskazuje w jakiej formie Prezes UKE będzie rozstrzygał o zasadności sprzeciwu.  **(31.)** Naszym zdaniem powinna to być decyzja administracyjna (jako władcza forma działania administracji). | **Uwaga nieuwzględniona**  Wprowadzenie decyzji administracyjnej jako instytucji prawnej wysoko sformalizowanej przy sprzeciwie od uznania SMSza smishing jest skrajnie nieadekwatne biorąc pod uwagę m.in. skalę. CSIRT NASK od kwietnia 2021 r. do końca maja 2020 r. zidentyfikował ok 31 000 złośliwych wiadomości sms. Dla przykładu załóżmy, że od 1% tych wiadomości zostałby złożony sprzeciw. Oznaczałoby to 310 postępowań administracyjnych prowadzonych przez Prezesa UKE. Byłoby to znaczne obciążenie organizacyjne dla tego organu.  Co istotne, odformalizowana procedura sprzeciwu zapewni szybkość procedowania sprawy. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 6 ust. 1 pkt 1 | **Art. 6 ust. 1 pkt. 1**  Trudno doprawdy zrozumieć czemu ma służyć określenie terminu 14- dniowego na rozpatrzenie sprzeciwu przez Prezesa UKE w stosunku do podstawowego terminu na rozpoznanie sprawy przez organ administracji publicznej wynoszący jeden miesiąc (art. 35 § 3 in principio k.p.a.).  Tym bardziej regulacja ta pozbawiona jest jakiegokolwiek znaczenia, skoro jeśli Prezes UKE uzna sprawę za szczególnie skomplikowaną, wówczas w świetle regulacji art. 35 § 3 k.p.a. może uznać, że ma na jej rozpoznanie 2 miesiące.  Ponadto należy podkreślić, że organ administracji publicznej, zwany dalej o.a.p., w przypadku niezałatwienia sprawy administracyjnej w terminie ustawowym obowiązany jest jedynie informację o niezałatwieniu sprawy w terminie przekazać do strony postepowania informując zarazem o przyczynach zwłoki w jej załatwieniu(z winy organu) lub też nawet wówczas, gdy uchybienie terminowi załatwienia sprawy nastąpiło z przyczyn od organu niezależnych (art. 36 k.p.a.).  W przypadku z kolei złożenia wniosku o ponowne rozpatrzenie sprawy Prezes UKE ma kolejny miesiąc na rozpatrzenie takiego wniosku (art. 35 § 3 in fine k.p.a. w zw. z art. 127 § 3 k.p.a.), a w razie niezałatwienia sprawy w terminie ustawowym Prezes UKE będzie zobowiązany do zawiadomienia storn postępowania o przyczynie niezałatwienia tej sprawy w terminie (art. 36 k.p.a.).  Po rozpatrzeniu sprawy przez prezesa UKE jako przez organ odwoławczy decyzja może być zaskarżona do wojewódzkiego sądu administracyjnego(art. 3 § 2 pkt. 1 p.p.s.a.), a postępowanie sądowoadministracyjne jest postępowaniem dwuinstancyjnym(art. 176 ust. 1 Konstytucji RP).  Skrócenie zatem w kwestionowanym przepisie terminu na rozpatrzenie przez Prezesa UKE sprzeciwu do 14 dni w rzeczywistości nie ma żadnego znaczenia, skoro SMS w tym czasie cały czas jest zablokowany (art. 4 ust. 6 pkt. 1 projektu, art. 7 projektu).  **Termin 14- dniowy na rozpatrzenie sprawy przez Prezesa UKE miałby jakikolwiek sens, gdyby z niezałatwieniem sprawy w terminie projektodawca powiązałby określone skutki prawne, przykładowo wskazując pod postacią obowiązku odblokowania SMS- a przez przedsiębiorcę telekomunikacyjnego lub też uznania z mocy prawa wniesionego przez nadawcę SMS- a sprzeciwu za uzasadniony**.  Takie jak ostatnio zaproponowane rozwiązanie nie byłoby odosobnione na gruncie prawa polskiego albowiem w art. 44 ust. 7 ustawy z dnia 29.12.1992 r. o radiofonii i telewizji (tekst jedn. Dz. U. z 2020 r. poz. 805 z późn. zm.), zwanej dalej ustawą o rtv, ustawodawca przewiduje, że jeżeli Przewodniczący Krajowej Rady Radiofonii i Telewizji w terminie miesiąca od dnia zgłoszenia nie odmówił rejestracji programu rozprowadzanego w rejestrze programów telewizyjnych nadawanych wyłącznie w systemie teleinformatycznym oraz programów rozprowadzanych, wówczas operator może legalnie rozpocząć rozprowadzanie takiego programu. | **Wyjaśnienie**  Wskazanie 14 dni na rozpatrzenie sprawy jest motywowane faktem, że sprzeciw nie ma charakteru decyzji administracyjnej, a więc nie będą stosowały się do niego przepisy KPA. Wprowadzenie instytucji zbliżonej do „milczącej zgody” mogłoby doprowadzić do sytuacji, że organ w przypadku wystąpienia dużej liczby sprzeciwów mógłby w sposób milczący uwzględnić sprzeciwy przestępców. Takie rozstrzygnięcie byłoby nieakceptowalne i podważałoby cel ustawy. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art.. 6 ust. 1 pkt 2 | **Art. 6 ust. 1 pkt 2**  Odnośnie przedmiotowej regulacji wskazać należy, że skoro Prezes UKE rozpoznając sprzeciw wydaje decyzję administracyjną (art. 104 § 1 k.p.a. w zw. z art. 206 ust. 1 prawa telekomunikacyjnego), to na zupełnym nieporozumieniu zasadza się wprowadzanie w kwestionowanym przepisie jakiejś odrębnej, poza doręczeniem decyzji administracyjnej, informacji o sposobie rozpatrzenia sprzeciwu.  I tak istotne w tej sprawie nie będzie doręczenie tego rodzaju pozbawionej skutków prawnych informacji lecz doręczenie ostatecznej decyzji administracyjnej wydanej po rozpoznaniu wniosku o ponowne rozpatrzenie sprawy lub niezaskarżonej tymże środkiem odwoławczym z art. 127 § 3 k.p.a., natomiast w przypadku wniesienia skargi do sądu administracyjnego na ostateczną decyzję Prezesa UKE istotne będzie dopiero wydanie wyroku prawomocnego, którym może być w razie wniesienia skargi kasacyjnej wyrok Naczelnego Sądu Administracyjnego, a co najmniej wyrok Wojewódzkiego Sądu Administracyjnego w warszawie.  **Z przytoczonych powyżej względów natury prawnej z uwagi na pozbawioną jakiegokolwiek znaczenia prawnego informację uregulowaną w art. 6 ust. 1 pkt. 2 projektu proponujemy wykreślenie normy art. 6 ust. 1p kt. 2 projektu jako normy pozbawionej jakiegokolwiek znaczenia prawnego regulującej sytuację prawnie nieistotną**. | **Wyjaśnienie**  Do sprzeciwu nie będą stosowane przepisy KPA. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 6 ust. 2 | **Art. 6 ust. 2**  Regulacja art. 6 ust. 2 projektu budzi kilka wątpliwości natury prawnej.  Po pierwsze, przewiduje iż w przypadku uwzględnienia sprzeciwu przez Prezesa UKE CSIRT NASK przekazuje informację o tym, że treść zawarta we wzorcu wiadomości stworzonym przez CSIRT NASK nie stanowi smishingu lub że niecelowe jest dalsze blokowanie SMS-ów zgodnie z wzorcem opracowanym przez CSIRT NASK.  Regulacja taka jest o tyle zaskakująca, że o ile można by ją uznać za uzasadnioną w sytuacji, gdy sprzeciw został wniesiony z tego powodu, że krótka wiadomość tekstowa została uznana za spełniającą znamiona smishingu zgodnie z wzorcem opracowanym przez CSIRT NASK (art. 4 ust. 6 pkt. 1 projektu), o tyle zupełnie niezrozumiałe jest przekazywanie tego rodzaju informacji przez CSIRT NASK w sytuacji gdy przedsiębiorca telekomunikacyjny zablokował SMS- a uznając go za wyczerpującego znamiona smishingu określone w art. 3 ust. 1 pkt. 2 projektu, mimo iż nie została tego rodzaju treść SMS-a ujęta we wzorcu opracowanym przez CSIRT NASK (art. 7 projektu).  Trudno zrozumieć dlaczegóż to CSIRT NASK miałby kogokolwiek informować o uwzględnieniu sprzeciwu przez Prezesa UKE, w sytuacji gdy sprzeciw nie był wniesiony w związku z faktem, że treść SMS-a spełniała wymogi smishingu określone we wzorcu przygotowanym przez CSIRT NASK albowiem należy zauważyć, że sprzeciw wnoszony jest przez nadawcę SMS-a wobec uznania jego treści za wyczerpującą znamiona smishingu niezależnie od tego czy przedsiębiorca telekomunikacyjny opierał się w swojej ocenie na wzorcu opracowanym przez CSIRT NASK(art. 4 ust. 6 pkt. 1 projektu), czy też na definicji legalnej przewidzianej w art. 3 ust. 1 pkt.2 projektu w sytuacji nieobjęcia treści konkretnego SMS-a wzorcem opracowanym przez CSIRT NASK (art. 7 projektu)[art. 5 ust. 1 projektu].  Po drugie, skoro stronami postępowania administracyjnego wszczętego wniesionym sprzeciwem jest nadawca krótkiej wiadomości tekstowej oraz przedsiębiorca telekomunikacyjny, który uznał konkretną wiadomość za spełniającą znamiona smishingu (art. 5 ust. 1 projektu w zw. z art. 28 k.p.a.), to zupełnie niezrozumiałe jest nałożenie na CSIRT NASK obowiązku powiadomienia konkretnych podmiotów o treści informacji ujętej w art. 4 ust. 5 projektu, skoro podmiot ten nie będąc stroną postepowania administracyjnego wszczętego wniesionym sprzeciwem nie posiada żadnej wiedzy o rozstrzygnięciu takiej sprawy przez Prezesa UKE.  Po trzecie wreszcie, regulację art. 6 ust. 2 projektu uznać należy także częściowo za absurdalną.  Absurdalność tej regulacji zasadza się w tym, że na okoliczność uwzględnienia sprzeciwu przez Prezesa UKE nakładając na CSIRT NASK obowiązek przekazania informacji określonej w art. 4 ust. 5 projektu podmiotom wymienionym w art. 4 ust. 3 projektu dochodzi do przekazania tej informacji Prezesowi UKE, który uwzględnił sprzeciw oraz przedsiębiorcy telekomunikacyjnemu, który zablokował SMS-a uznając, że spełnia wymogi smishingu określone w wadliwym wzorcu stworzonym przez CSIRT NASK, a zatem tym podmiotom, które doskonale wiedzą, że w oparciu o wzorzec opracowany przez CSIRT NASK niezasadne będzie uznawanie krótkich wiadomości tekstowej za spełniające znamiona smishingu, gdyż właśnie z tego powodu Prezes UKE sprzeciw nadawcy SMS-a uwzględnił.  **Propozycja zmiany tego przepisu zmierza do:**  **a/ wprowadzenia w tym przepisie obowiązku poinformowania przez Prezesa UKE CSIRT NASK o uwzględnieniu sprzeciwu od uznania przez przedsiębiorcę telekomunikacyjnego krótkiej wiadomości tekstowej za spełniającą znamiona smishingu dokonanego w oparciu o wzorzec stworzony przez CSIRT NASK,**  **b/wyłączenia obowiązku przekazania przez CSIRT NASK informacji określonej w art. 4 ust. 5 projektu Prezesowi UKE oraz przedsiębiorcy telekomunikacyjnemu, który był stroną postępowania administracyjnego, w którym Prezes UKE decyzją ostateczną uwzględnił sprzeciw wniesiony przez nadawcę SMS-a**. | **Uwaga częściowo uwzględniona**  Sprzeciw będzie przysługiwał w sytuacji, gdy przedsiębiorca telekomunikacyjny zablokował SMS zgodnie ze wzorcem.  Do postępowania ws. rozpatrzenia sprzeciwu nie będą stosowane przepisy KPA.  Przepisy ustawy wyraźnie wskazują, że użytkownicy będą mogli zgłaszać sprzeciw do Prezesa UKE i przez to wskazywać, że wzorzec przygotowany przez NASK jest niedoskonały. W przypadku gdy Prezes UKE uwzględni sprzeciw, CSIRT NASK będzie musiał zmienić swój wzorzec. Będzie to skuteczny sposób podważania wzorca smishingu. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 7 | **VIII. [BLOKOWANIE SMS WYCZERPUJĄCYCH ZNAMIONA SMISHINGU, INNE NIŻ ZAWARTE REJESTRZE – ART. 7]**  **(32.)** Pragniemy podkreślić, że w tym zakresie Projektodawca przewidział pewną swobodę. Niemniej jednak w takim przypadku przedsiębiorca nie powinien ponosić żadnej odpowiedzialności (o charakterze publicznoprawnym ani wobec użytkowników).  Wnosimy zatem o wyłączenie takich konsekwencji. | **Uwaga nieuwzględniona**  W tym przypadku nie jest zasadne wprowadzanie regulacji o charakterze szczególnym. Przedsiębiorca telekomunikacyjny niezasadnie blokujący SMS na podstawie art. 7 będzie podlegał odpowiedzialności kontraktowej za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 7 | **Izba sprzeciwia się proponowanej w art. 7 projektu regulacji w zakresie, w którym uprawnienie przedsiębiorców telekomunikacyjnych (a właściwie operatorów sieci mobilnych) do blokowania także takich SMS, które nie są zawarte we wzorcu opracowanym przez CSIRT NASK nie podlegało żadnej kontroli**.  Przede wszystkim projekt ustawy nie określa żadnych środków odwoławczych od decyzji przedsiębiorcy telekomunikacyjnego ani nawet możliwości kontroli przez organy publiczne kryteriów stosowanych przez te podmioty do oceny treści. Generalnie każdy MNO będzie mógł dowolnie blokować SMS przychodzące nie tylko od jego klientów, ale przede wszystkim z sieci innych przedsiębiorców telekomunikacyjnych lub urządzeń integratorów SMS, w dodatku bez żadnej kontroli i konsekwencji. Regulacja ta spowoduje problemy z interoperacyjnością usług SMS pomiędzy podmiotami biorącymi udział w ich przesyłaniu oraz blokowanie SMS, które nie są smishingiem. Generalnie Izba zwraca uwagę, że to uprawnienie przyznane MNO stoi w sprzeczności z regulacją o roli CSIRT NASK jako instytucji monitorującej smishing i inicjującej reakcję na nowe przypadki czy z rolą Prezesa UKE jako organy decydującego czy dany SMS jest smishingiem czy nie (art. 6 projektu). Izba wskazuje, że w przypadku wątpliwości co do SMS nieodpowiadających treści wzorców CSIRT NASK, należy co najmniej przeprowadzić konsultacje robocze z podmiotem, z którego sieci/urządzenia taki SMS został wysłany, czy też zawiadomić o tym CSIRT NASK i Prezesa UKE. Izba wskazuje, że poleganie na systemach automatycznie blokujących połączenia głosowe czy przesyłanie SMS rodzi wiele nieporozumień i częstego blokowania prawidłowych usług. Z tego względu na rynku przyjęto zasadę analizy wątpliwych przypadków przez wyznaczonego pracownika przedsiębiorcy telekomunikacyjnego lub nawet spotkań roboczych w celu omówienia wątpliwości przed podjęciem decyzji o zablokowaniu kwestionowanej usługi. Proponowana w ustawie regulacja uniemożliwia „ludzką” analizę usług telekomunikacyjnych i konsultacje międzyoperatorskie lub z klientem w przypadku kwestionowanego komunikatu.  Niezależnie od wprowadzenia postulowanych przez KIKE zmian wynikających z konieczności wprowadzenia nadzoru nad stosowaniem uprawnień przez przedsiębiorców telekomunikacyjnych, należy dodać zapisy o odpowiedzialności MNO za blokowanie SMS nie będących smishingiem zarówno w formie kar finansowych jak i formie odszkodowawczej. W przypadku nadużywania przez MNO uprawnienia z art. 7 projektu Prezes UKE mógłby nakazać modyfikację wykorzystywanego systemu stosującego wadliwą identyfikację smishingu. Izba wskazuje, że taką karą finansową mogłaby być 50-krotność opłaty za zablokowane SMSy niebędące smishingiem (taką stawkę stosują operatorzy w przypadku nadużycia telekomunikacyjnego związanego z podmianą numeru A abonenta wywołującego). | **Wyjaśnienie**  Przedsiębiorca telekomunikacyjny niezasadnie blokujący SMS na w zw. z projektowanym uprawnieniem o charakterze uzupełniającym będzie podlegał odpowiedzialności kontraktowej za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 7 wz z art. 4 ust. 6 pkt 1 | **Art. 7 oraz art. 4 ust. 6 pkt. 1**  Art. 7 projektu oraz art. 4 ust. 6 pkt. 1 projektu dają przedsiębiorcy telekomunikacyjnemu bardzo szerokie uprawnienia kontroli wszystkich SMS-ów przesyłanych w jego sieci telekomunikacyjnej i blokowania tych SMS-ów, które zdaniem przedsiębiorcy telekomunikacyjnego spełniają znamiona smishingu, czy to przewidziane we wzorcu stworzonym przez CSIRT NASK, czy też nieobjęte tym wzorcem..  Aby zidentyfikować SMS podlegający blokowaniu przedsiębiorca telekomunikacyjny za pomocą systemu informatycznego musi skontrolować („przeczytać”) wszystkie SMS-y przesyłane w sieci telekomunikacyjnej, przeanalizować ich treść, ocenić ich treść pod kątem zgodności z definicją smishingu oraz ze wzorcem opracowanym, przez CSIRT NASK, a następnie zablokować te SMS, które przedsiębiorca uzna za „wyczerpujące znamiona smishingu”.  Wobec bardzo szerokiej i niejednoznacznej definicji smishingu zawartej w art. 3 ust. 1 pkt 2 projektu przy jednoczesnej niemożności zastosowania wzorca przedsiębiorca telekomunikacyjny może blokować SMS według własnego wzorca informacji wyczerpującej znamiona smishingu.  **Poważnie należy się zastanowić, czy przyznanie przedsiębiorcy telekomunikacyjnemu tak daleko idących kompetencji ingerowania w treść wszystkich sms- ów przechodzących w jego sieci telekomunikacyjnej nie została zbyt daleko posunięta**. | **Uwaga wyjaśniona**  Przepisy projektu nie zwalniają przedsiębiorcy telekomunikacyjnego z obowiązku ochrony tajemnicy telekomunikacyjnej. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 8 | **IV. [ŚRODKI NIEZBĘDNE W CELU ZAPOBIEGANIA CLI SPOOFINGU – ART. 8]**  **(15.)** Przepis art. 8 stanowi o obowiązku blokowania połączeń głosowych.  **(16.)** Wskazujemy, że **przedsiębiorcy telekomunikacyjni zrzeszeni w Izbie nie wiedzą w jaki sposób identyfikować połączenia noszące znamiona CLI spoofing**.  Niezbędnym jest wypracowanie i zdefiniowanie metod identyfikacji zachowań noszących znamiona CLI spoofing.  **(17.)** Otwartymi pozostają pytania:  1) czy przedsiębiorca będzie ponosił odpowiedzialność za niezasadne zablokowanie połączeń (chodzi w tym o odpowiedzialność publicznoprawną oraz wobec abonenta)?  W tym kontekście w Prezentacji wskazano na następujące wątpliwości:  „*co w przypadku, gdy zablokowany lub ograniczany będzie ruch legalny? Kto decyduje o jego „nielegalnym” charakterze? Czy w ogóle dokonanie takiej oceny jest możliwe?*”  „*czy możliwość ograniczenia ruchu dotyczyć będzie wyłącznie pojedynczego użytkownika czy całego ruchu w przypadku jego tranzytu/roamingu?*”  2) jaki będzie nadzór Prezesa UKE nad realizacją tego obowiązku.  **(18.)** Jeszcze raz powołujemy się w tym zakresie na Prezentację. MC jako argument dla krytyki jednej z propozycji Rynku wskazał, że „*definicja posługuje się nieostrymi pojęciami, brak jest wyraźnie stypizowanych i konkretnych zachowań kwalifikujących je jako nadużycie telekomunikacyjne*”.  Obecnie projektowana propozycja nie sprostała ww. wymaganiom prezentowanym przez ówczesne MC.  **(19.)** Jak się wydaje, służyć ma temu wypracowanie przez Prezesa UKE z przedsiębiorcami telekomunikacyjnymi „*środków organizacyjnych i technicznych, które* (przedsiębiorcy – dopisek) *będą stosowali przy realizacji obowiązków, o których mowa w art. 8*” (art. 10 ust. 1 Projektu).  Jednakże zwracamy uwagę, że Projekt wskazuje na fakultatywność zawarcia tego porozumienia, a ponadto porozumienie może być zawarte z niektórymi przedsiębiorcami (którzy niekoniecznie mogą być zainteresowani problemem nadużyć).  **(20.)** Z drugiej strony niewykonywanie obowiązku, o którym mowa w art. 8 jest penalizowane (z tym, że kara ma być fakultatywna).  **(21.)** Przedsiębiorca telekomunikacyjny z reguły dowiaduje się o połączeniu o charakterze CLI spoofingu ex post (po jego wykonaniu). Tym bardziej niezrozumiałe jest wprowadzenie obowiązku blokowania połączeń.  **(22.)** Jednocześnie podkreślamy, że nie rozumiemy sensu anonimizacji połączeń (przedsiębiorca „*ukrywa identyfikację numeru wywołującego dla użytkownika końcowego*”).  **(23.)** W konsekwencji wnosimy alternatywnie o:  1) wprowadzenie fakultatywnego blokowania połączeń (oraz wyłączenie penalizowania takiego typu naruszenia) (jako rozwiązanie docelowe lub przejściowe) albo  2) określenie metod identyfikacji zachowań spełniających znamiona CLI spoofingu oraz proporcjonalnych środków technicznych i organizacyjnych służących do zwalczania tego zjawiska przez akt o charakterze normatywnym albo  3) wprowadzenie postulowanego przez Rynek zakazu wykorzystywania numeracji nie przyznanej (w bramkach internetowych) oraz ustawowego obowiązku niezmienności numeru A na całej drodze połączenia (co faktycznie powinno wyłączyć połączenia o cechach CLI spoofingu).  Propozycja przepisów [rozwiązanie 1) i 2)]:  ***Art. 8.*** *1. W celu zapobiegania i zwalczania wykrytych przez przedsiębiorcę telekomunikacyjnego przypadków CLI spoofing przedsiębiorca telekomunikacyjny blokuje takie połączenie głosowe. W takim przypadku użytkownikowi nie przysługuje jakiekolwiek odszkodowanie.*  *2. Minister właściwy do spraw cyfryzacji określi, w drodze rozporządzenia, sposoby identyfikacji zachowań posiadających znamiona CLI spoofing oraz środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w ust. 1*.  Przepis przejściowy:  ***Art. YYY****. Do czasu wejścia w życie rozporządzenia, o którym mowa w art. 8 ust. 2 w celu zapobiegania i zwalczania wykrytych przypadków CLI spoofing przedsiębiorca telekomunikacyjny może zablokować takie połączenie głosowe. W takim przypadku użytkownikowi nie przysługuje jakiekolwiek odszkodowanie.* | **Uwaga nieuwzględniona**  Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym a Prezesem UKE.  Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń.  Dzięki takiemu rozwiązaniu przedsiębiorcy telekomunikacyjni wraz ze wsparciem i nadzorem UKE będą mogli wypracować najlepsze rozwiązania techniczne i organizacyjne, które pozwolą im zwalczać nadużycia w komunikacji elektronicznej. Bezpieczeństwo regulacyjne w przypadku prawidłowego wykonywania porozumienia da odpowiednią korzyść do pracy nad porozumieniem i jego wdrożeniem.  Dla mniejszych przedsiębiorców telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków które będę określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało ich odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych przedsiębiorców. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 8 | W art. 8 projektu ustawy jako formę zwalczania spoofingu nakazuje się samodzielne blokowanie połączeń głosowych przez operatora (bez żadnych trybów czy interwencji UKE/NASK) lub ukrycie identyfikacji numeru wywołującego. **Izba wskazuje po pierwsze, że regulacja ta jest korzystna wyłącznie dla dużych operatorów, którzy na tej postawie będą mogli blokować kwestionowany przez siebie ruch telekomunikacyjny (bez względu czy jest on nadużyciem telekomunikacyjnym czy nie).** Po drugie jest ona błędna w kwestiach technicznych. Blokowanie połączeń ma być realizowane (jako obowiązek a nie uprawnienie) w celu zapobiegania i zwalczania spoofingu. Nie jest jasne jaka jest równica między zapobieganiem a zwalczaniem. Wg Izby istnieje zagrożenie, że w celu zapobiegania spoofingowi dopuszczalne będzie blokowanie prezencyjne połączeń z określonych punktów styku, określonej numeracji czy z określonego zakończenia sieci bez względu czy faktycznie jest to spoofing czy nie. Izba wskazuje, że przepis ten powinien umożliwiać blokowanie tylko takich połączeń, które są spoofingiem. Przedsiębiorca telekomunikacyjny z kolei ma pewność, że dane połączenie jest spoofingiem wyłącznie, jeśli jest ono inicjowane w jego własnej sieci (wie, że to zakończenie sieci ma inny numer niż wykazywany w systemie). Z tego względu przepis ten powinien uprawniać przedsiębiorców telekomunikacyjnych do blokowania połączeń ze spoofingiem tylko jeśli są inicjowane z jego własnej sieci. W przypadku połączeń spoza jego sieci operator nie będzie miał takiej wiedzy i może to stwierdzić dopiero post factum badając rekordy ze swojego punktu styku.  Za całkowicie wadliwe należy uznać mechanizm przeciwdziałania spoofingowi polegający na ukrywaniu identyfikacji numeru wywołującego. Po pierwsze jest to możliwe tylko w przypadku połączeń w obrębie jednej sieci telekomunikacyjnej. Zgodnie z zasadami międzyoperatorskimi połączenie głosowe przychodzące na punkt styku bez numeru A abonenta wywołującego jest automatycznie traktowane jako fraudowe i blokowane na punkcie styku (lub też rozliczane jako oszustwo międzyoperatorskie z ciężkimi karami finansowymi). Żaden więc przedsiębiorca telekomunikacyjny nie będzie mógł ukryć identyfikację numeru wywołującego. | **Uwaga nieuwzględniona**  Projektowany art. 8 musi być odczytywany wraz z art. 3 definiującym to nadużycie oraz art. 10 mówiącym o porozumieniu oraz rekomendacjach Prezesa UKE. Mniejsi operatorzy telekomunikacyjni, którzy nie będą mogli dołączyć do porozumienia z prezesem UKE, będą mogli oprzeć swoje działania na rekomendacjach Prezesa UKE określających środki organizacyjne i techniczne, które powinny być stosowane przy wykonywaniu obowiązku określonego w art. 8. Co istotne prawidłowe stosowanie rekomendowanych środków będzie zwalniało z odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej będące skutkiem wprowadzonych tych środków. Rekomendacje te będą dostosowane do możliwości technicznych operatorów.  W zakresie ukrywania identyfikacji numeru wywołującego obowiązek ten dotyczy jedynie ukrycia identyfikacji przed użytkownikiemkońcowym a nie przed innym operatorem. |
|  | Polska Izba Komunikacji Elektronicznej | Art. 8 | **Sposoby zapobiegania i zwalczania spoofingu *(art. 8)***  Projekt ustawy przewiduje nałożenie na przedsiębiorców telekomunikacyjnych obligatoryjnych dwóch sposobów zapobiegania i zwalczania CLI spoofing. Tymi sposobami są blokowanie połączenia głosowanego i ukrywanie identyfikacji numeru wywołującego dla użytkownika końcowego.  **Izba negatywnie ocenia proponowane rozwiązanie.**  W pierwszej kolejności wskazać należy, że ustawa nie powinna ograniczać katalogu środków stosowanych w ramach zapobiegania i zwalczania CLI spoofing. Spowodowane jest to przede wszystkim możliwością stosowania innych, równie skutecznych mechanizmów działania. *Ratio legis* wprowadzenia tego przepisu jest klarowne – ustawa ma wprowadzić narzędzie możliwie skuteczne, aby zapobiegać naruszeniom. W opinii Izby natomiast, wykładnia projektowanego przepisu nakazuje przyjąć, że wprowadza on **katalog zamknięty** stosowanych środków. Wynika to przede wszystkim z tego, że przepis wprowadza obowiązek ich stosowania przez przedsiębiorców telekomunikacyjnych.  Zdaniem Izby, wprowadzenie katalogu zamkniętego środków zapobiegania i zwalczania CLI spoofing nie będzie rozwiązaniem optymalnym. **W dalszych pracach nad ustawą powinno się rozważyć zastąpienie katalogu zamkniętego tych mechanizmów katalogiem otwartym, które umożliwi ich dostosowanie do możliwości technicznych i finansowych przedsiębiorców telekomunikacyjnych**.  Po drugie, art. 8 należy koniecznie doprecyzować wskazaniem, że jakiekolwiek działania przedsiębiorców telekomunikacyjnych powinny następować *ex post*, a zatem dopiero po wykryciu przypadków CLI spoofing. Działania nie powinny być oparte o abstrakcyjną analizę potencjalnych przypadków nadużycia, w szczególności o automatyczne modele predykcyjne, ale powinny dotyczyć takich przypadków, w których naruszenia byłyby dostatecznie **zweryfikowane**. Należy zatem wziąć pod rozwagę, że rozwiązania *ex ante* mogą nie być rozwiązaniem optymalnym. Przepisy nie powinny ponadto pozostawiać tak szerokiego zakresu swobody doboru środków działania, który pozwalałby wykorzystywać przewidziane w przepisach mechanizmy do nieuczciwych praktyk konkurencyjnych.  Wprowadzenie obowiązku stosowania działań mających na celu jedynie zapobieganie CLI spoofing rodzi poważne **ryzyko nadużywania regulacji**. W szczególności ryzyko to odnosi się do podejmowania działań wobec właściwych ruchów w sieci tytułem zapobiegania tym niewłaściwym. To z kolei może przerodzić się w praktyce w liczne spory między operatorami telekomunikacyjnymi, a nawet w spory z abonentami.  W dalszej mierze podkreślić należy, że art. 8 skonstruowany jest niezwykle szczątkowo, co sprzyja niewłaściwej wykładni nałożonych na przedsiębiorców telekomunikacyjnych obowiązków. Prawidłowe zastosowanie tego przepisu mogłoby zostać zapewnione wyłącznie poprzez jego doprecyzowanie. Konieczność doprecyzowania tym bardziej uzasadnia penalizacja niewykonywania obowiązków, o których mowa w art. 8, na mocy art. 15 ust. 2 pkt 2). | **Uwaga wyjaśnienie**  Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym w Prezesem UKE. Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 8 | **ad Art. 8.** W celu zapobiegania i zwalczania CLI spoofing przedsiębiorca telekomunikacyjny blokuje połączenie głosowe albo *ukrywa identyfikację numeru wywołującego* dla użytkownika końcowego.  Propozycja PTI  Zamienić cały powyższy przepis na poniższy:  *W celu zapobiegania i zwalczania odbioru połączeń z szalbierczych numerów dzwoniących przedsiębiorca telekomunikacyjny blokuje połączenie głosowe i podaje informację o zablokowaniu połączenia i jego przyczynie.*  Komentarz PTI  Ukrycie identyfikacji szalbierczego numeru wywołującego nie tylko nie wystarczy, ale doprowadzi do skutku przeciwnego niż zamierzony przez regulację – połączenie będzie odbierane bez świadomości szalbierstwa. | **Uwaga nieuwzględniona**  Ukrycie numeru ma nastąpić w sytuacji gdy przedsiębiorca telekomunikacyjny ma wątpliwości czy połączenie nie jest spoofowane, ale tej pewności nie ma. Użytkownik końcowy widząc taką informację (a w zasadzie jej brak) powinien nabrać wątpliwości co do tego połączenia. Część odbiorców nie odbierze takiego połączenia, a pozostali mimo tego, że odbiorą, będą moglinabrać wątpliwości, dlaczego np. znajoma osoba albo osoba podająca się za pracownika instytucji – policji, banku – dzwoni z numeru prywatnego. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 8 | **Art. 8**  Art. 8 projektu daje przedsiębiorcy telekomunikacyjnemu bardzo szerokie uprawnienia dotyczące blokowania połączeń głosowych  Przedsiębiorca telekomunikacyjny samodzielnie podejmuje decyzję o zablokowania połączenia głosowego. Przed zablokowaniem połączenia głosowego musi stwierdzić, że użytkownik wywołujący połączenie głosowe nie jest uprawniony do posługiwania się „informacją adresową” (niezdefiniowana w projekcie) wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik.  Dalej przedsiębiorca musi jednoznacznie stwierdzić, że to połączenie głosowe służy podszyciu się pod inny podmiot niż ww. użytkownik. Następnie przedsiębiorca telekomunikacyjny musi jednoznacznie zbadać cel wykonania połączenia i po stwierdzeniu, że takim celem jest nakłonienie odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing) blokuje takie połączenie.  Stwierdzenie „podszywania” się użytkownika wywołującego pod numer telefoniczny należący do innego użytkownika jest czynnością techniczną i może to być wykonane za pomocą sytemu informatycznego bez potrzeby większej ingerencji w połączenia.  Wskazanie, że jest to połączenie głosowe „służące podszyciu się pod inny podmiot w celu nakłonienia odbiorcy tego połączenia do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji oprogramowania (CLI spoofing).”, wykonane przed zestawieniem połączenia, zdaniem opiniujących jest niemożliwe.  Podkreślić należy, że aby przedsiębiorca mógł legalnie zablokować połączenie muszą być spełnione wszystkie przesłanki zawarte w definicji CLI spoofingu (art. 3 ust. 1 pkt 3 projektu).  **Pojawia się zatem pytanie, czy w omawianym przypadku nie mamy do czynienia z przepisem niemożliwym do zrealizowania w praktyce, co świadczyłoby o nieracjonalności ustawodawcy (projektodawcy), a co świadczyłoby o obrazie konstytucyjnej zasady demokratycznego państwa prawnego (art. 2 Konstytucji RP).** | **Wyjaśnienie**  Nieuprawnione modyfikowanie informacji adresowej (nie tylko w kontekście CLI Spoofing) również zostało uznane za nadużycie w komunikacji elektronicznej. Rozmowy przeprowadzone z przedsiębiorcami telekomunikacyjnymi wskazują, że będą oni w stanie rozpoznawać tak zdefiniowane nadużycia i im przeciwdziałać. Nie można też zgodzić się, że przedsiębiorcy telekomunikacyjni będą mieli tak duży zakres swobody przy blokowaniu połączeń. Wciąż będą oni związani postanowieniami umownymi, a nieprawidłowe zablokowanie wiadomości będzie wiązało się z odpowiedzialnością umowną. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 9 | Izba popiera tworzenie przez Prezesa UKE wykazu numerów, z których nie mogą być inicjowane połączenia telefoniczne z art. 9 projektu ustawy. Jest to metoda, której domagają się sami członkowie Izby oraz ich klienci. Regulacja ta wymaga jednak kilku poprawek. Po pierwsze, wykaz nie powinien być publikowany w biuletynie informacji publicznej UKE, gdyż wymagałoby to podłączenie do niego systemów każdego przedsiębiorcy telekomunikacyjnego i ręcznego monitorowania wykazu. Zamiast tego wykaz ten powinien być częścią systemu PLI CBD, zarządzającego lokalizacją numeracji i jej przenoszenia, do którego systemu każdy przedsiębiorca już jest podłączony (i to w dodatku automatycznie zaciągane są dane). Rozwiązanie to będzie praktyczniejsze i tańsze. Po drugie, w ust. 3 powinno być uprawnienie przedsiębiorców telekomunikacyjnych oraz ich użytkowników do wpisywania numerów usług infolinii i biura obsługi klienta wykorzystywanych przez użytkowników a nie przez samych przedsiębiorców telekomunikacyjnych. Jednocześnie Izba wskazuje, że w art. 9 ust. 9 projektu ustawy powinien być zapis o wniosku o usunięciu numeru z wykazu Prezesa UKE zamiast o wycofaniu wniosku o wpis tego numeru. Taka regulacja jest bardziej elastyczna zwłaszcza w przypadku przeniesienia numeru do innego operatora lub zmian właścicielskich w firmie dysponującym numerem wpisanym do wykazu. Postępowanie o usunięcie numeru z wykazu odbywałoby się samodzielnie bez konieczności „kontynuowania” postępowania o umieszczenie numeru w wykazie. | **Uwaga nieuwzględniona**  Przyjęte procedury zapewniają również efektywność obsługi wniosków o wpis do wykazu.  Zakres podmiotów mogących wnioskować o wpis jest ukształtowany od strony świadczącego usługę (usługodawcy), a nie korzystającego z niej (usługobiorcy). Biorąc pod uwagę pożądany skutek i cel ustawy jest to rozwiązanie właściwe.  Proponowane procedury związane z działaniem wykazu mają zapewnić efektywne wykonywanie zadań przez UKE. Taka forma wykazu jest najłatwiejsza do wdrożenia (od integracji z PLICBD czy PIT jak wskazuje UKE). |
|  | Polska Izba Komunikacji Elektronicznej | Art. 9 | **Wykaz numerów telefonów służących wyłączenie do odbierania połączeń głosowych *(art. 9)***  W odniesieniu do propozycji wprowadzenia jawnego wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych Izba nie zgłasza stanowczo negatywnych uwag.  PIKE zgłasza jedynie prośbę o przedstawienie motywów wprowadzenia wykazu wraz z wizją jego zastosowania w praktyce, w szczególności przez przedsiębiorców telekomunikacyjnych. Poza tym, zgłaszamy również potrzebę przedstawienia przez projektodawcę sposobu synchronizacji systemów przedsiębiorców telekomunikacyjnych z tym wykazem.  Powyższa prośba uzasadniona jest szczególnie przez nieprecyzyjną konstrukcję przepisów i zawarte w nich błędy legislacyjne (np. art. 9 ust. 3). Ponownie dostrzegamy potrzebę przygotowania przepisów klarownych, by ograniczyć wątpliwości interpretacyjne. Uwaga ta odnosi się do art. 9 w całości. | **Uwaga wyjaśniona**  Rozwiązanie pozwoli skutecznie zapobiegać połączeniom spoofingowym z numerów, które zostaną umieszczone w wykazie. Połączenia z wykorzystaniem takiego numeru będą przerywane przez przedsiębiorców telekomunikacyjnych i nie zostaną terminowane u użytkownika końcowego – projekt przewiduje blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu. Szczególnie istotne jest, że kluczowe instytucje finansowe takie jak banki zamieszczą swoje numery w tym wykazie. Ich numery są często wykorzystywane przez przestępców aby wzbudzić zaufanie i wprowadzić w błąd już od momentu odebrania połączenia przez użytkownika końcowego. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 9 ust. 1 | **Wykaz numerów służących wyłącznie do odbierania połączeń**  Projektowana ustawa zakłada, że Prezes UKE będzie prowadził wykaz numerów, które służą wyłącznie do odbierania połączeń (art. 9 ust. 1 projektu ustawy). Przedsiębiorcy telekomunikacyjni mają blokować połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu (art. 9 ust. 12 projektu ustawy). Jednocześnie projektowana ustawa zakłada, że Prezes UKE będzie mógł nałożyć karę pieniężną za naruszenie przez przedsiębiorcę telekomunikacyjnego obowiązku blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu (art. 15 ust. 2 pkt 3) projektu ustawy).  Jeśli przedsiębiorcy telekomunikacyjni mają działać w reżimie obowiązku, pod groźbą kary (nawet jeśli ma to być kara fakultatywna) to konieczne będzie uzupełnienie przepisów projektowanej ustawy o regulacje, które precyzyjnie określają w jaki sposób Prezes UKE będzie udostępniał informacje zawarte w wykazie (na stronie internetowej, poprzez system informatyczny, inaczej), jak również o przepisy określające, ile czasu - od momentu przekazania informacji przez Prezesa UKE o wpisie do wykazu - ma przedsiębiorca telekomunikacyjny na zaimplementowanie w swojej sieci i rozpoczęcie blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu. Mechanizm taki musi:   * być niezawodny i dostępny, aby każdy przedsiębiorca telekomunikacyjny w kraju mógł wywiązać się z obowiązku; * być racjonalny kosztowo, zarówno z perspektywy kosztów, jakie poniesie Prezes UKE na stworzenie i utrzymanie wykazu jak i z perspektywy kosztów, jakie będą musieli ponieść przedsiębiorcy telekomunikacyjni na wdrożenie i utrzymanie rozwiązania; * dawać przedsiębiorcom telekomunikacyjnych czas niezbędny na pobranie informacji z wykazu oraz jej implementację w sieciach telekomunikacyjnych i rozpoczęcie blokowania; termin na wykonanie obowiązku – liczony od momentu przekazania przez Prezesa UKE informacji o wpisie numeru do wykazu – nie może być krótszy niż 3 dni robocze; * komunikacja z wykazem powinna dawać się automatyzować (oczywiście z uwzględnieniem postulatu racjonalności kosztów), co oznacza, że nawet jeśli komunikacja z wykazem przyjmie postać pobierania pliku ze strony Prezesa UKE, to nie należy stosować rozwiązań takich jak CAPTCHA, uniemożliwiających automatyzację procesu.   Powyższe wymagania muszą być spełnione, jeśli przedsiębiorcy telekomunikacyjni mają działać w reżimie obowiązku pod groźbą kary. Brak przepisów precyzujących powyższe zagadnienia spowoduje, że ani Prezes UKE ani przedsiębiorcy telekomunikacyjni nie będą wiedzieli, czy w danym przypadku powstaje już zagrożenie karą czy nie.  Szczegółowe określanie na poziomie ustawy zasad funkcjonowania wykazu nie będzie jednak konieczne, jeśli Projektodawca, zgodnie z naszym ogólnym postulatem, zastąpi obowiązek uprawnieniem do blokowania połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu albo co najmniej, jeśli Projektodawca (pozostawiając reżim obowiązku) zrezygnuje z możliwości nakładania kary pieniężnej za niewykonanie tego obowiązki. Zatem alternatywnie, w stosunku do postulatu uzupełnienia projektu ustawy o szczegółowe zasady funkcjonowania wykazu, proponujemy usunięcia z projektu ustawy art. 15 ust. 2 pkt 3) (przewidującego możliwość nałożenia kary za niewywiązanie się z analizowanego obowiązku). | **Uwaga częściowo uwzględniona**  Projektodawca przewiduje, że wykaz numerów, które służą wyłącznie do odbierania połączeń będzie prowadzony za pomocą systemu teleinformatycznego i będzie miał on charakter rejestru publicznego.  Ponadto obowiązek przedsiębiorcy telekomunikacyjnego został doprecyzowany: „Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu do wykazu, blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do wykazu.”.  **W zakresie zmiany obowiązku na uprawnienie po stronie przedsiębiorców telekomunikacyjnych i kwestii kar**  Projektowane rozwiązania, po uwzględnieniu uwag, są wystarczające precyzyjnie. Aby skutecznie walczyć z nadużyciami w komunikacji elektronicznej powinien zostać nałożony obowiązek prawny (obowiązki) na przedsiębiorców telekomunikacyjnych. W przypadku przyznania uprawnienia przedsiębiorca telekomunikacyjny mógłby, ale nie musiałby podejmować działań mających na celu zwalczanie nadużyć. Natomiast ryzyko nałożeniu sankcji w przypadku niewypełnienia obowiązków m.in. realizuje funkcję prewencyjną i represyjną. |
|  | Związek Banków Polskich | Art. 9 ust. 1-4 , 6-9 i 12 oraz ust. 13 (nowy) | 1. Prezes UKE, prowadzi jawny wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych **oraz wykaz** **numerów służących do inicjowania połączeń głosowych** i udostępnia je w Biuletynie Informacji Publicznej na swojej stronie podmiotowej.   2. Prezes UKE dokonuje wpisu do wykazów, o których mowa w ust. 1, na wniosek:  1) jednostki sektora finansów publicznych, o której mowa w art. 9 z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz. U. 2021 r. poz. 305, z późn. zm.)),  2) banku  **3) spółdzielczej kasy oszczędnościowo-kredytowej**  **4) centrum analizy i wymiany informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)**  **5) podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczeństwa, w rozumieniu ustawy z dnia 5 lipca 2018 r. o Krajowym Systemie Cyberbezpieczeństwa (Dz.U. z 2020 r. poz. 1369 z późn. zm.)**  3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykaz**ów**, o których mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii.  4. Wniosek, o którym mowa w ust. 2 i 3, zawiera wskazanie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych **lub numeru służącego do inicjowania połączeń głosowych**  6. Prezes UKE dokonuje wpisu numeru do wyka**zów**, o któr**ych** mowa w ust. 1, w terminie 5 dni od dnia otrzymania wniosku.  7. Wpis do wyka**zów**, o któr**ych** mowa w ust. 1, jest czynnością materialno-techniczną.  8. Prezes UKE odmawia wpisu do wyka**zów**, o który**ch** mowa w ust. 1, w drodze decyzji, jeżeli wniosek został złożony przez podmiot nieuprawniony lub dotyczy on numeru niewykorzystywanego przez ten podmiot.  9. Podmiot, który złożył wniosek, o którym mowa w ust. 2 i 3, może w każdym czasie go wycofać. W takim przypadku Prezes UKE niezwłocznie, jednak nie później niż w terminie 5 dni od dnia złożenia wniosku o wycofanie numeru z wykazu, wykreśla numer z wyka**zów**, o który**ch** mowa w ust. 1.  12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia inicjowane z wykorzystaniem numeru wpisanego do **wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych.**  13. **Przedsiębiorca telekomunikacyjny obowiązany jest do podjęcia szczególnych działań organizacyjnych i technicznych służących zapobieganiu oraz zwalczaniu CLI spoofing wykonywanego przy wykorzystaniu numerów wskazanych w wykazie numerów służących do inicjowania połączeń głosowych**  W opinii sektora bankowego stworzenie rejestru numerów służących wyłącznie do odbierania połączeń (oraz zobowiązanie przedsiębiorców telekomunikacyjnych do blokowania połączeń wychodzących z tych numerów) może okazać się niewystarczające. W związku z powyższym, proponujemy stworzenie drugiego rejestru, który zawierałby numery zgłoszone przez wymienione podmioty, charakteryzujące się kluczowym znaczeniem dla działalności danego podmiotu (np. numery centrali telefonicznej, infolinii, działu bezpieczeństwa itp.). Jednocześnie, przedsiębiorca telekomunikacyjny powinien w przypadku tych numerów (umożliwiających również wykonywanie połączeń wychodzących) podejmować nadzwyczajne środki przeciwdziałające występowaniu zjawiska spoofingu. Praktyka pokazuje, że znaczna część przestępstw spoofingowych jest popełniania przy wykorzystaniu właśnie tego rodzaju numerów, umożliwiających wykonywanie połączeń wychodzących.  Proponujemy również uwzględnienie w przedmiotowym katalogu instytucji uprawnionych do zgłaszania numerów do obu wykazów, spółdzielczych kas z uwagi na charakter działalności tego rodzaju podmiotów, który może być wykorzystywany do nadużyć w komunikacji elektronicznej.  Ponadto, proponujemy uwzględnienie w katalogu, instytucji tworzonych przez banki wspólnie z bankową izbą gospodarczą – tj. centrum wymiany i analiz informacji, których tworzenie byłoby możliwe na podstawie znowelizowanych przepisów ustawy - Prawo Bankowe wskazanych poniżej, a także podmioty wchodzące w skład Krajowego Systemu Cyberbezpieczeństwa. Wskazane podmioty były celem ataków spofingowych/vishingowych i jako instytucje zaufania publicznego były i mogą być narażone na materializację ryzyka utraty reputacji. | **Uwaga częściowo uwzględniona w zakresie dodania SKOK do listy podmiotów uprawnionych do wpisu do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych.  W pozostałym zakresie uwaga nieuwzględniona**  W pozostałym zakresie należy zauważyć, że obecne zasady związane z funkcjonowaniem tego rejestru są w wystarczający sposób określone w ustawie.  Chcemy aby do rejestru były wpisane podmioty, których numery szczególnie często są wykorzystywane przez przestępców. Są to przede wszystkim podmioty z sektora finansowego. W związku z tym niecelowe byłoby dołączenie do wykazu podmiotów krajowego systemu cyberbezpieczeństwa.  Równocześnie obowiązek zwalczania spoofingu, zwłaszcza blokowania połączeń jest już zawarty w przygotowywanej ustawie jak choćby w projektowanym art. 8. Zgodnie z zasadami techniki prawodawczej nie należy powtarzać norm prawnych. |
|  | Związek Telewizji Kablowych Izba Gospodarcza | Art. 9 ust. 1 | **Art. 9 ust. 1**  Prezes UKE prowadzi wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych wykorzystywanych przez jednostki sektora finansów publicznych, banki lub przez przedsiębiorców telekomunikacyjnych.  Jest to w rzeczywistości niewielki tylko odsetek wszystkich numerów telefonów, które mogą być wykorzystane do nadużyć.  **Sugeruje się zatem rozszerzenie katalogu podmiotów, które mogą zgłosić swoje numery telefonów wykorzystywanych wyłącznie do odbierania połączeń głosowych**. | **Uwaga uwzględniona**  Katalog podmiotów uprawnionych do złożenia przedmiotowego wniosku zostanie rozszerzony m. in. o SKOK. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 9 ust. 3 | **Wpis numeru do wykazu numerów służących wyłącznie do odbierania połączeń**  Projektowana ustawa w art. 9 ust. 3 przewiduje możliwość wpisu numeru do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych, oraz wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby biura obsługi klientów lub infolinii. Takiego wpisu dokonuje Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego,.  Rozumiemy, iż intencją ustawodawcy jest, aby przedsiębiorcy telekomunikacyjni zyskali możliwość wpisania do wykazu numerów własnych wykorzystywanych w swojej działalności biznesowej do kontaktu klientów z przedsiębiorcą, np. w celach obsługowych. W przeszłości zdarzały się również przypadki podszywania się oszustów pod takie numery biura obsługi klientów lub infolinii.  W ramach Izby, otrzymaliśmy sygnały, iż wskazany przepis może być interpretowany i wykorzystany przez klientów, w szczególności klientów B2B z którymi przedsiębiorca ma zawarte umowy o świadczenie usług, jako obowiązek zgłaszania przez przedsiębiorcę telekomunikacyjnego numerów udostępnionych tym klientom (w ramach świadczonych usług) i wykorzystywanych przez klientów na potrzeby biura obsługi klientów lub infolinii. W ocenie Izby, aby uniknąć tych wątpliwości, przepis należy doprecyzować tak, aby mówił o numerach wykorzystywanych przez przedsiębiorcę na potrzeby własne biura obsługi klientów lub infolinii.  *3. Prezes UKE na wniosek przedsiębiorcy telekomunikacyjnego dokonuje wpisu do wykazu, o którym mowa w ust. 1, wyłącznie numerów wykorzystywanych przez przedsiębiorcę telekomunikacyjnego na potrzeby własne biura obsługi klientów lub infolinii.*  Jeżeli projektodawca ocenia jednak, iż istniałaby potrzeba, aby do wykazu numerów służących wyłączenie do odbierania połączeń głosowych wpisywały się także inne podmioty niż wskazane w art. 9 ust. 2, warto rozważyć dodanie zapisów, które to uwzględnią. Inne podmioty mogłyby dopisywać się do takiego wykazu, jeżeli wykazałyby Prezesowi UKE np. swój interes faktyczny. | **Uwaga częściowo uwzględniona** Przepis zostanie dookreślony poprzez dodanie „własne”. |
|  | Krajowa Izba Gospodarcza Elektroniki i Telekomunikacji | Art. 9 ust. 12 | **X. [BLOKOWANIE POŁĄCZEŃ – ART. 9 UST. 12]**  **(36.)** Proponujemy zmianę zapisów w art. 9 ust 12, który dotyczy sposobu postępowania z połączeniami wykonywanymi z numerów umieszczonych w wykazie numerów. Przedsiębiorca telekomunikacyjny powinien blokować połączenia **przychodzące** do jego sieci z numerów telefonów służących wyłącznie do odbierania połączeń głosowych. Połączenia z tych numerów nie będą inicjowane. Wiele przypadków spoofingu dotyczy połączeń tranzytowanych i przychodzących z sieci innych operatorów.  *„12. Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych blokuje połączenia przychodzące z wykorzystaniem numeru wpisanego do wykazu.”* | **Uwaga uwzględniona**  Przepis został zmieniony zgodnie z uwagą, że mowa jest o połączeniach przychodzących. „Przedsiębiorca telekomunikacyjny świadczący usługę połączeń głosowych niezwłocznie, nie później niż w terminie 3 dni od dnia wpisu do wykazu, blokuje połączenia przychodzące do jego sieci z wykorzystaniem numeru wpisanego do wykazu.”. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 10 | W art. 10 wprowadza się w fakultatywne porozumienie przedsiębiorcy telekomunikacyjnego z Prezesem UKE o środkach technicznych i organizacyjnych zwalczania spoofingu, które pozwala na zwolnienie od odpowiedzialności za blokowane połączenia telefoniczne w ramach walki ze spoofingiem. Regulacja ta budzi poważne zastrzeżenia Izby biorąc pod uwagę jej ogólny i niejasny charakter z ogromnymi konsekwencjami. Nie jest jasne jak miałoby wyglądać takie porozumienie, z iloma podmiotami i jak bardzo musiałoby być szczegółowe. Z uwagi na zwolnienie od odpowiedzialności za blokowanie ruchu, porozumienie to powinno być zarówno bardzo szczegółowe jak też jawne, gdyż będzie ono elementem sporów międzyoperatorskich. Przykładowo operator A zablokuje ruch telekomunikacyjny od operatora B, argumentując, że robi to w celu zapobiegania spoofingowi i robi to zgodnie z zawartym przez siebie porozumieniem z Prezesem UKE. Tymczasem operator B nie może zweryfikować tych twierdzeń, czy porozumienie operatora A z Prezesem UKE rzeczywiście uprawnia do dokonanej blokady ruchu. Co więcej, porozumienie to zwalnia operatora A od odpowiedzialności względem operatora B za zablokowanie legalnego ruchu. Biorą pod uwagę praktykę zawierania porozumień przez Prezesa UKE tylko z dużymi podmiotami gospodarczymi, regulacja ta doprowadzi do dyskryminacji tych przedsiębiorców telekomunikacyjnych, którzy nie zawrą porozumienia z Prezesem UKE (w pierwszej kolejności MŚP, a więc członków KIKE). Izba postuluje rezygnację z porozumień z Prezesem UKE na rzecz niedyskryminacyjnych i proporcjonalnych regulacji ogólnorynkowych oraz zwolnienie od odpowiedzialności wyłącznie za zablokowanie usług, które faktycznie były nadużyciem. Dodatkowo wątpliwości Izby budzi zakres podmiotowy art. 10 ust. 1 projektu, gdzie wskazuje się, że porozumienie z Prezesem UKE w zakresie spoofingu mogą zawrzeć tylko operatorzy, a nie dostawcy usług komunikacji głosowej. | **Uwaga wyjaśniona**  Ustawa będzie wskazywać, że porozumienie z Prezesem UKE mogą zawrzeć operatorzy świadczący usługi telekomunikacyjne dla co najmniej 50 000 abonentów. Do pozostałych operatorów telekomunikacyjnych Prezes UKE będzie mógł skierować rekomendacje określające środki organizacyjne i techniczne. Kwestie szczegółowe związane z porozumieniem nie powinny znaleźć się w ustawie ze względu na swój techniczny charakter i zostaną doprecyzowane w ramach współpracy między UKE a przedsiębiorcami.  Projektodawca proponuje, aby środki techniczne i organizacyjne mające na celu zapobieganie i zwalczanie CLI spoofing były doprecyzowane w porozumieniu zawartym z Prezesem UKE.  Ten model samoregulacji ma z jednej strony zapewnić bezpieczeństwo regulacyjne dla przedsiębiorców telekomunikacyjnych, a z drugiej jest on na tyle elastyczny, aby można było dostosować środki do ciągle rozwijających się nowych technologii jak i zagrożeń.  Dzięki takiemu rozwiązaniu przedsiębiorcy telekomunikacyjni wraz ze wsparciem i nadzorem UKE będą mogli wypracować najlepsze rozwiązania techniczne i organizacyjne, które pozwolą im zwalczać nadużycia w komunikacji elektronicznej. Bezpieczeństwo regulacyjne w przypadku prawidłowego wykonywania porozumienia da odpowiednią korzyść do pracy nad porozumieniem i jego wdrożeniem.  Dla mniejszych przedsiębiorców telekomunikacyjnych, którzy mogliby nie być w stanie wypełnić obowiązków które będę określone w porozumieniu, Prezes UKE będzie wydawał rekomendacje. Prawidłowe wykonywanie rekomendacji Prezesa UKE będzie wyłączało ich odpowiedzialności za niewykonanie lub nienależyte wykonanie usługi telekomunikacyjnej tych przedsiębiorców. |
|  | Polska Izba Komunikacji Elektronicznej | Art. 10 | **Porozumienie w zakresie realizacji obowiązków, o których mowa w art. 8 *(art. 10)***  W zakresie możliwości zawarcia porozumienia między operatorem a Prezesem UKE PIKE nie zgłasza negatywnych uwag. Zwracamy jednak uwagę, że zmianę należy wprowadzić w OSR projektu, ze względu na konieczność wprowadzenia zmian w regulaminach rozpatrywania reklamacji przez przedsiębiorców telekomunikacyjnych w przypadku zawarcia porozumienia. | **Uwaga uwzględniona**  W OSR zostanie uwzględniona stosowna wzmianka. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 11 | W art. 11 ust. 2 wprowadza się fakultatywne porozumienie przedsiębiorcy telekomunikacyjnego z Prezesem UKE w zakresie domen internetowych służących do spoofingu oraz fakultatywną możliwość blokowania dostępu do takich domen. Projekt ustawy tego nie precyzuje, ale uprawnienie do blokowania wskazanych domen internetowych dotyczy przede wszystkim dostawców dostępu do sieci Internet, a nie samych dostawców usług głosowych. Biorąc pod uwagę poziom wiedzy technicznej oszustów korzystających ze spoofingu proponowany mechanizm będzie nieskuteczny i należy z niego zrezygnować (np. korzystanie z VPN). Ponadto mechanizm ten jest pozbawiony kontroli innych rejestrów zablokowanych domen i może poradzić do blokowania domen niezwiązanych z realnymi nadużyciami w komunikacji elektronicznej. Obecny zapis jest tak szeroki i niejasny, że może pod niego podlegać np. Facebook, Twitter, allegro czy każdy sklep internetowy. | **Uwaga nieuwzględniona**  Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[[3]](#footnote-4). |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 11 | **Lista ostrzeżeń NASK**  Art. 11 ust. 6 projektu ustawy stanowi, że przedsiębiorca telekomunikacyjny może uniemożliwić dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1 art. 11. Przy obecnym brzmieniu może powstać wątpliwość, czy przedsiębiorca telekomunikacyjny będzie mógł uniemożliwić dostęp do domen obecnych na liście CSIRT NASK, ale należących do zakresu domen wskazanych w ust. 2 art. 11 (skoro przepis upoważniający do uniemożliwienia dostępu referuje do ust. 1 w art. 11 projektu ustawy).  W ocenie Izby, aby uniknąć tych wątpliwości, analizowany przepis należy doprecyzować tak, aby odsyłał do listy, o której mowa w ust. 3 (a nie ust. 1):  *Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 3.*  To właśnie ust. 3 w art. 11 projektu ustawy mówi o liście prowadzonej przez CSIRT NASK (a na listę tę składają się dwa zakresy domen, wymienione w ust. 1 i 2 w art. 11). | **Uwaga uwzględniona** |
|  | Polska Izba Komunikacji Elektronicznej | Art. 11 | **Porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych *(art. 11)***  Art. 11 projektu przewiduje możliwość zawarcia fakultatywnego porozumienia w zakresie prowadzenia i utrzymywania:  1) jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu (ust. 1)  2) jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron (ust. 2)  oraz uniemożliwienia dostępu do tych stron.  Izba przede wszystkim zgłasza swoje wątpliwości co do zasadności prowadzenia wskazanych powyżej list ostrzeżeń w proponowanym kształcie. Przeszkodą w praktycznym zastosowaniu tych list i uniemożliwiania dostępu do poszczególnych stron jest bowiem brak dostosowania do realnych nadużyć. Podkreślenia wymaga fakt, że podmioty doprowadzające do nadużyć w komunikacji elektronicznej posługują się szeroką wiedzą oraz zaawansowanymi technologiami. Z tego względu należy stwierdzić, że **przedmiotowa regulacja nie sprosta wyzwaniom stawianym przez strony internetowe służące do wyłudzania danych i środków finansowych.** | **Uwaga nieuwzględniona**  Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[[4]](#footnote-5). |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 11 ust. 1 | **ad Art. 11. ust. 1.** W celu ochrony użytkowników internetu przed stronami internetowymi wyłudzającymi dane, w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia  i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwienia dostępu do tych stron.  Propozycja PTI zmiany treści zapisu:  *W celu ochrony użytkowników internetu przed szalbierczymi stronami internetowymi wyłudzającymi dane,w tym dane osobowe oraz doprowadzającymi użytkowników internetu do niekorzystnego rozporządzenia ich majątkiem, może zostać zawarte porozumienie w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących szalbierczych stron internetowych oraz uniemożliwienia do nich dostępu.*  Komentarz PTI  Takimi szalbierczymi stronami mogą być tylko niektóre strony z danej domeny. Wobec tego blokowanie całej domeny jest działaniem nadmiarowym – należy się ograniczyć tylko do blokowania stron. | **Uwaga nieuwzględniona**  Praktyka pokazuje, że z reguły niebezpieczne są całe domeny. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 11 ust. 2 | **ad Art. 11. ust.2.** W celu ochrony użytkowników internetu przed CLI spoofing, elementem porozumienia, o którym mowa w ust. 1, może być jawna lista ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron.  Komentarz PTI  Ten ustęp jest zbędny, gdyż CLI spoofing dotyczy połączeń głosowych a nie stron internetowych, chyba że chodzi tutaj o strony internetowe, które służą podmianie lub ukryciu prawdziwego numeru dzwoniącego. W tym przypadku można je po prostu uznać za strony szalbiercze i potraktować jak te z ust.1. Ale też przy istnieniu VPN uniemożliwianie dostępu do tych stron może być mało skuteczne. | **Uwaga wyjaśniona**  W tym przepisie chodziło o domeny, za pomocą których oszuści dokonują CLI spoofing. Ze względu na odmienny, bardziej skomplikowany charakter decyzji o wpisie takich domen do listy, proponuje się usunięcie regulacji projektowanego art. 11 ust. 2. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 11 ust. 3, 4, 5, 6 | **ad Art. 11 ust 3. , 4., 5., 6.**  Propozycja PTI zmiany treści zapisu:  W tych ustępach należy wpisać strony internetowe, a nie domeny internetowe. | **Uwaga nieuwzględniona**  Praktyka pokazuje, że z reguły niebezpieczne są całe domeny. |
|  | Związek Banków Polskich | Art. 11 ust. 4 | 4. Stronami porozumienia są:  1) Prezes UKE;  2) minister właściwy do spraw informatyzacji;  3) Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy, oraz  4) przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni,  **5) centrum analizy i wymiany informacji utworzone na podstawie art. 106 ust. 6 ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)**  Postulujemy uwzględnienie w katalogu podmiotów będących stronami porozumienia dotyczącego zgłaszania domen internetowych, instytucji tworzonych przez banki wspólnie z bankową izbą gospodarczą – tj. centrum wymiany i analiz informacji. FinCERT.pl – BCC ZBP jako reprezentant sektora finansowego winien mieć możliwość w imieniu np. banków wnioskowania o prowadzenie do rejestru zidentyfikowanych przestępczych domen. Taka możliwość usprawni przepływ informacji z i w ramach sektora finansowego. | **Uwaga nieuwzględniona w związku z nieuwzględnieniem zmian w Prawie bankowym** |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 11 ust. 5 | **ad Art. ust.5** Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady zgłaszania domen internetowych, wpisania oraz usuwania ich z listy ostrzeżeń, o której mowa w ust. 1.  Propozycja PTI zmiany treści zapisu – należy go zmodyfikować jak poniżej:  *Porozumienie określa co najmniej zasady współpracy między stronami, w tym zasady i podstawy zgłaszania, wpisania, blokowania oraz zwalniania stron internetowych z listy ostrzeżeń, o której mowa w ust. 1.*  Komentarz PTI  Uważamy, iż przyczyny powodujące zgłoszenie muszą być jawne, gdyż łączne z proponowaną zmianą w ust. 6 art. 11 nie spowoduje to dezorientacji użytkownika w sytuacji odmowy świadczenia usługi dostępu do konkretnej strony. Ponadto proponowane uzupełnienie zapobiegnie arbitralnemu blokowaniu dostępu do stron internetowych. | **Uwaga wyjaśniona**  Art. 11 ust. 5 zawiera otwarty katalog elementów, które ma regulować porozumienie. Jest to minimalny zakres porozumienia. Nie ma potrzeby uszczegóławiania tego przepisu, tym bardziej, że propozycja PTIIR również zmierza do określenia katalogu otwartego. Ponadto, proponuje się, aby uprawnienie dot. sprzeciwu umieszczeniu domeny na liście ostrzeżeń wynikało wprost z przepisów rangi ustawowej. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 11 ust. 6 | **ad Art. 11 ust. 6.** Przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom internetu dostęp do stron internetowych wpisanych na listę, o której mowa w ust. 1.  Propozycja PTI  Należy dodać przed końcową kropką poniższy fragment:  *, wraz z podaniem przyczyny blokady.*  Komentarz PTI  W związku w danym przepisem w przypadku zaakceptowania propozycji PTI powyżej do art. 11 ust. 1 powyższy przepis nie spowoduje dezorientacji użytkownika końcowego, gdyż odmowa świadczenia usługi (blokada) będzie umotywowana prawnie, ale nie technicznie, np. w postaci kodów błędów protokołu http. | **Uwaga nieuwzględniona**  Przepis to norma zobowiązująca przedsiębiorcę telekomunikacyjnego do podjęcia określonego działania w przypadku tych domen, które zostały umieszczone na liście ostrzeżeń. Nie ma potrzeby jego doprecyzowywania. |
|  | IAB Polska | Art. 12 ust. 1 pkt 1 w związku z art. 2 pkt 15 | **UWAGA:**  Wątpliwości budzi definicja użytkownika, odwołująca się do definicji z ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne (art. 2 pkt 49). Zgodnie z definicją z Prawa telekomunikacyjnego użytkownikiem jest „*podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi*”.  Odwołanie się do definicji z Prawa telekomunikacyjnego jest **niewłaściwe**, ponieważ **usługa poczty elektronicznej nie jest publicznie dostępną usługą telekomunikacyjn**ą, a jak – sama definicja poczty elektronicznej określa (art. 2 pkt 8 UZNKE) – jest to „*usługa komunikacji interpersonalnej niewykorzystująca numerów*”, a więc żadna **osoba korzystająca z usługi poczty elektronicznej nie może być uznana za użytkownika w rozumieniu tej definicji**.  **PROPOZYCJA:**  IAB Polska proponuje, aby projektodawca zaproponował inną definicję użytkownika, która będzie adekwatna w stosunku do usług, z jakich użytkownicy będą korzystali. | **Uwaga uwzględniona**  Przepisy zostały zmienione tak, że nie mówią już o „użytkowniku” a o „użytkowniku poczty”, co mityguje ryzyko niewłaściwej interpretacji. |
|  | IAB Polska | Art. 12 ust. 1 pkt 3 | **UWAGA:**  Z UZNKE nie wynika, **co należy rozumieć przez „*aktywne konto pocztowe***”, czym jest konto pocztowe i kiedy konto pocztowe należy uznać za aktywne lub nieaktywne.  Ponadto dostawca poczty elektronicznej, który spełnia przesłankę posiadania 500 000 użytkowników określoną w art. 12 ust. 1 pkt 1 UZNKE, będzie najczęściej spełniać przesłankę posiadania 500 000 aktywnych kont pocztowych (jeśli za aktywne konto pocztowe uzna się np. konto, z którego można wysyłać i odbierać e-maile). Użytkownik konta pocztowego będący osobą fizyczną najczęściej korzysta tylko z jednego konta pocztowego, zatem sama przesłanka posiadania przez dostawcę poczty elektronicznej 500 000 użytkowników powinna być wystarczająca dla oceny, czy dostawca poczty elektronicznej powinien spełniać obowiązki określone w art. 12 UZNKE.  **PROPOZYCJA:**  IAB Polska proponuje wykreślenie z art. 12 ust. 1 UZNKE pkt 3: „*obsługujący co najmniej 500 000 aktywnych kont pocztowych*”. | **Uwaga uwzględniona**  Zostanie usunięte odwołanie „aktywnego konta pocztowego”. |
|  | IAB Polska | Art. 12 ust. 1 | **UWAGA:**  Art. 12 ust. 1 UZNKE wskazują, że dostawca poczty elektronicznej będzie zobowiązany stosować jednocześnie trzy mechanizmy uwierzytelniania poczty elektronicznej (DMARC – Domain-based Message Authentication Reporting and Conformance, DKIM – DomainKeys Identified Mail oraz SPF – Sender Policy Framework). Z kolei z uzasadnienia do projektu UZNKE wynika, że dostawcy poczty elektronicznej będą mieli obowiązek stosować jeden z tych mechanizmów, co oznacza, że być może na poziomie redakcji tekstu UZNKE **powstała nieścisłość konieczna do skorygowania**.  **PROPOZYCJA:**  IAB Polska wnosi – zgodnie z przedstawioną poniżej propozycją art. 12 ust. 1 UZNKE, aby dostawca poczty elektronicznej nie był zobowiązany do stosowania łącznie wszystkich mechanizmów uwierzytelniania poczty elektronicznej, a jedynie **jeden z tych wskazanych w art. 12 ust. 1 UZNKE, wybrany samodzielnie przez dostawcę poczty elektroniczne**j.  *Art. 12. 1. Dostawca poczty elektronicznej:*  *1) dla co najmniej 500 000 użytkowników,*  *2) dla podmiotu publicznego, lub*  *~~3) obsługujący co najmniej 500 000 aktywnych kont pocztowych~~*  *– ma obowiązek stosowania jednego z następujących mechanizmów: SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance)* ***lub*** *DKIM (DomainKeys Identified Mail).* | **Uwaga wyjaśniona**  Uzasadnienie zostanie skorygowane.  Zamiarem projektodawcy jest, aby dostawcy poczty elektronicznej stosowali wszystkie 3 wskazane mechanizmy co ograniczy zjawisko spoofowania emaili. |
|  | Nazwa.pl sp. z o.o. | Art. 12 | Z uzasadnienia do Projektu ustawy wynika, że celem projektu ustawy jest wprowadzenie odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Z założenia, *„proponowane rozwiqzania majq służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolq w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników".*  Z uwagi na powyższe, w Projekcie ustawy przewidziano obowiązek wprowadzenia określonych mechanizmów uwierzytelniania poczty elektronicznej przez następujących dostawców poczty elektronicznej: (1) dla co najmniej 500 000 użytkowników, (2) dla 500 000 aktywnych kont pocztowych, lub (3) dla podmiotów publicznych.  Jednocześnie z Oceny Skutków Regulacji wynika, że na etapie projektowania ustawy nie zgromadzono informacji o liczbie dostawców poczty elektronicznej, którzy zostaną objęci nowymi regulacjami. Potwierdza to fakt, że w tabeli w pkt 4 Oceny Skutków Regulacji dotyczącej podmiotów, na które oddziałuje Projekt ustawy, przy oznaczeniu dostawców poczty elektronicznej widnieje informacja: *„brak danych".*  Tymczasem w ocenie Spółki przewidziany w Projekcie ustawy próg 500 000 (użytkowników lub aktywnych kont pocztowych) jest zdecydowanie zbyt wysoki, przez co nowe obowiązki wynikające z Projektu ustawy mogłyby dotyczyć jedynie bardzo niewielkiego fragmentu rynku dostawców poczty elektronicznej.  Spółka wskazuje, że dla dalszych prac nad Projektem ustawy przydatnym może być aktualizowany na bieżąco (ostatnia aktualizacja z dnia 7 lipca 2022 roku) ranking firm hostingowych w Polsce dostępny pod adresem toplOO.webhostingtalk.pl, prowadzony przez webhostingtalk.pl spółka z ograniczoną odpowiedzialnością (KRS: 0000695069) - por. kopia rankingu firm hostingowych w Polsce toplOO.webhostingtalk.pl stanowiąca załącznik do niniejszego pisma.  Mając na uwadze powyżej przywołany ranking, w ocenie Spółki uzasadnionym byłoby, aby w miejsce przewidzianego w Projekcie ustawy progu 500 000 (użytkowników lub aktywnych kont pocztowych) wprowadzić próg 50 000 (użytkowników lub aktywnych kont pocztowych).  Alternatywnie można rozważyć również powiązanie nowych obowiązków z liczbą domen, dla których serwer podmiotu będącego dostawcą usługi poczty elektronicznej jest autorytatywny -tutaj Spółka proponuje próg 25 000 nazw domen, dla których serwer dostawcy usługi poczty elektronicznej jest autorytatywny.  Jako dodatkowe uzasadnienie wskazać można, że na mocy ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa w związku z rozporządzeniem Rady Ministrów w sprawie wykazu usług kluczowych oraz progów istotności skutku zakłócającego incydentu  dla świadczenia usług kluczowych, za dostawcę usługi kluczowej w zakresie prowadzenia autorytatywnego serwera DNS może zostać uznany podmiot, który świadczy usługi DNS minimalnie dla 100 000 nazw domen, dla których serwer jest autorytatywny. W kontekście powyższego, w ocenie Spółki tym bardziej uzasadnione jest by obniżyć próg przewidziany w Projekcie ustawy, skoro przy obowiązkach wynikających z ustawy o krajowym systemie cyberbezpieczeństwa (o zdecydowanie większym ciężarze gatunkowym) przewidziano zdecydowanie mniejszy próg, uzależniony od liczby nazw domen, dla których serwer jest autorytatywny. Można dostrzec tutaj analogię do liczby użytkowników poczty elektronicznej lub aktywnych kont pocztowych, o których mowa w Projekcie ustawy.  Pozwoliłoby to wyeliminować negatywny efekt (jak można zakładać - nieoczekiwany przez projektodawcę) związany z objęciem nowymi regulacjami jedynie niewielkiego procentu podmiotów będących dostawcami komercyjnej usługi poczty elektronicznej, który to efekt w konsekwencji nie przyczyniłby się do zrealizowania założeń Projektu ustawy w zakresie znaczącego zwiększenia poziomu bezpieczeństwa w komunikacji elektronicznej. | **Uwaga wyjaśniona**  Przy projektowaniu regulacji konieczne jest zachowanie równowagi pomiędzy obowiązkami nakładanymi na dostawców poczty elektronicznej a środkami bezpieczeństwa. Nałożenie nowych obowiązków na wszystkich dostawców poczty elektronicznej mogłoby nieproporcjonalnie dotknąć małych i średnich przedsiębiorców. |
|  | Nazwa.pl sp. z o.o. | Art. 12 ust. 1 | Spółka pozytywnie ocenia przewidziany w Projekcie ustawy obowiązek wprowadzenia przez dostawców poczty elektronicznej mechanizmów SPF (Sender Privacy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail) oraz obowiązek korzystania z takich mechanizmów przez podmiot publiczny. Spółka jednocześnie rekomenduje, aby w sposób jednoznaczny wyjaśnić, że obowiązkowe jest stosowanie wszystkich trzech mechanizmów (jak wynika z Projektu ustawy), a nie tylko jednego z nich (jak wynika z uzasadnienia Projektu ustawy). Stosowanie tylko jednego z tych zabezpieczeń w sposób oczywisty nie chroni przed zagrożeniami, które stały się podstawą do przyjęcia Projektu ustawy.  Jednocześnie Spółka wskazuje, że w ocenie Spółki nieprawidłowym jest brak w Projekcie ustawy wymogu stosowania zabezpieczenia DNSSEC. Stosowanie DNSSEC powinno stać się - oprócz SPF, DMARC oraz DKIM - kluczowym filarem bezpieczeństwa w Internecie i rozwiązaniem służącym zwalczaniu nadużyć w komunikacji elektronicznej. W ocenie Spółki, weryfikowanie zabezpieczeń SPF/DKIM/DMARC, które opierają się na informacjach z DNS, z jednoczesnym pozostawieniem możliwości fałszowania informacji w DNS, nie będzie wystarczającą ochroną użytkowników. Z tego względu, w ocenie Spółki, Projekt ustawy powinien przewidywać również obowiązek stosowania rozwiązania zabezpieczającego przed możliwością fałszowania informacji przekazywanych przez system DNS, jakim jest uznawany powszechnie standard, tj. DNSSEC. | **Uwaga wyjaśniona**  W ocenie projektodawcy wskazywanie konkretnych rozwiązań w zakresie bezpieczeństwa jest techniką stosowaną tylko gdy jest to absolutnie niezbędne – tak jak w tym przypadku. Na podmiotach publicznych spoczywa również ogólny obowiązek zapewnienia bezpieczeństwa swoich systemów w tym poczty. W związku z tym popieramy stosowanie rozwiązania takiego jak DNSSEC, ale równocześnie nie chcemy narzucać go wszystkim podmiotom. |
|  | Unia Metropolii Polskich | Art. 12 | **Uwaga zasadnicza 1.** – przepis w naszej ocenie jest niezasadny oraz nie potrzebny. Odpowiednie wymagania w tym zakresie wynikają już z zasad oceny ryzyka z KRI dotyczących bezpieczeństwa informacji. Być może należy wzmocnić w tym zakresie przepisy KRI – które jak wiadomo nie zostały wdrożone w terminie. | **Uwaga nieuwzględniona**  Przepis ten przyczyni się do wzrostu bezpieczeństwa poczty elektronicznej. Należy też zaznaczyć, że kolejne przepisy precyzują rolę CSIRT NASK w tej kwestii:  „CSIRT NASK publikuje na swojej stronie internetowej informację na temat standardów sieciowych RFC (Request for Comments) z odniesieniem do dokumentów umieszczonych na stronach internetowych organizacji Internet Engineering Task Force, które składają się na aktualną wersję opisów mechanizmów SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail)." |
|  | Unia Metropolii Polskich | Art. 12 | **Uwaga zasadnicza 2.** Brak wskazania skutków finansowych dla wprowadzonych obowiązków. Czy i w jakim zakresie wpłynie to na koszt korzystania z usług. | **Uwaga wyjaśniona**  Należy zauważyć, że zaproponowane rozwiązania nie wiążą się z istotnym nakładem finansowym i nie powinny wymagać zatrudniania dodatkowych osób do ich skutecznego wprowadzenia, a ich wprowadzenie nie powinno zając więcej niż kilka dni roboczych. |
|  | Unia Metropolii Polskich | Art. 12 | Przepis jest nieprawidłowo skonstruowany. Obowiązki podmiotu publicznego powinny być zawarte w tym przypadku w ustawie stanowiącej podstawę działania podmiotów w tym zakresie albo w KSC albo chociażby w ustawie o informatyzacji. | **Uwaga nieuwzględniona**  Projektowany akt prawny znajduje się na styku dziedziny prawa telekomunikacyjnego i wyodrębniającego się materialnego prawa administracyjnego z zakresu cyberbezpieczeństwa. Z tego względu, a także ze względu na doniosłość materii regulowanej, zasadne jest aby przepisy te znalazły się w odrębnym akcie prawnym. |
|  | Unia Metropolii Polskich | Art. 12 | Przepis w naszej ocenie łamie zasadne neutralności technologicznej. Wymagania konkretne dot. Mechanizmów powinny być zawarte w rozporządzeniu. | **Uwaga nieuwzględniona**  Nie można zgodzić się z zaproponową zmianą. Należy podkreślić, że obowiązki powinny być nakładane w drodze ustawy, a nie rozporządzenia. Ponadto, wskazane w przepisie mechanizmy SPF, DKIM, DMARC są najbardziej rozpowszechnione. Przepis nie zabrania stosowania dodatkowo innych mechanizmów uwierzytelnienia. |
|  | Unia Metropolii Polskich | Art. 12 | Brak przepisu przejściowego dla podmiotów publicznych na dostosowanie się do tego wymagania. Obowiązek wchodzi włącznie z ustawą, co w przypadku krótkiego okresu nie jest w tym przypadku możliwe do dotrzymania. | **Uwaga częściowo uwzględniona**  Okres *vacatio legis* jest wystarczający na realizację nowych obowiązków. Ustawienie odpowiednich mechanizmów nie powinno zająć więcej niż kilka dni roboczych. |
|  | Unia Metropolii Polskich | Art. 12 | Przepis nie przewiduje skutków dla zobowiązań umownych wprowadzenia nowego obowiązku np. wygaśnięcia umów ex lege, podstawy do wypowiedzenia umowy bez terminu wypowiedzenia, lub innego mechanizmu dającego podmiotom publicznym szansę na dostosowanie się do nowego wymagania. | **Uwaga uwzględniona**  Zostanie dodany przepis przejściowy, zgodnie z którym dostawca poczty elektronicznej, który świadczy usługę poczty elektronicznej na podstawie umowy, której stroną jest podmiot publiczny, obowiązującej w dniu wejścia w życie ustawy, jest obowiązany w terminie 3 miesięcy od dnia wejścia w życie ustawy do spełnienia wymagań, o których mowa w art. 15 ust. 1.  2. Jeżeli dostawca poczty elektronicznej nie spełni wymagań w terminie, o którym mowa w ust. 1, umowa ulega może zostać jednostronnie rozwiązania przez podmiot publiczny a dostawcy poczty elektroniczne nie przysługują roszczenia z tego tytułu. |
|  | Unia Metropolii Polskich | Art. 12 | Prezes UKE ustrojowo nie jest podmiotem upoważnionym do prowadzenia takiej kontroli, gdyż nie jest ona prowadzona w stosunku do jst jako przedsiębiorcy telekomunikacyjnego. Ewentualna kontrola powinna być prowadzona nie przez podmiot regulacyjny a administracyjny. | **Uwaga nieuwzględniona**  Materia tego przepisu dotyczy kwestii komunikacji, która znajduje się we właściwości Prezesa Urzędu Komunikacji Elektronicznej. |
|  | Polskie Towarzystwo Informatyczne Izba Rzeczoznawców | Art. 12 ust. 1 | **ad Art. 12. ust. 1.** Dostawca poczty elektronicznej:  1) dla co najmniej 500 000 użytkowników,  2) dla podmiotu publicznego, lub  3) obsługujący co najmniej 500 000 aktywnych kont pocztowych  – ma obowiązek stosowania mechanizmu SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance) oraz DKIM (DomainKeys Identified Mail).  Propozycja PTI  Zmodyfikować zapis powyższego ustępu na poniższy (opis modyfikacji w komentarzu):  *Dostawca poczty elektronicznej:*  *1) dla co najmniej 500 000 użytkowników,*  *2) dla podmiotu publicznego, lub*  *3) obsługujący co najmniej 500 000 zarejestrowanych kont pocztowych*  *– jest zobowiązany do wyboru i do stosowania jednego lub wielu ze znanych mechanizmów potwierdzania wiarygodności podanego nadawcy mejla, w szczególności takich jak SPF (Sender Policy Framework), DMARC (Domain-based Message Authentication Reporting and Conformance), DKIM (DomainKeys Identified Mail).*  Komentarz PTI  Nie jest znana definicja, czym jest aktywne konto pocztowe. Wiele zarejestrowanych kont może być latami nieaktywnych, ale być dla ich właściciela użytecznymi. Jedynym kryterium dla obsługującego konta jest opłacenie lub spełnianie określonych wymagań. W związku z tym w propozycji zastąpiono określenie „aktywnych” na określenie „zarejestrowanych”.  W propozycji PTI nie ma wymuszania stosowania wymienionych mechanizmów (wszystkich lub jednego z nich, jak SPF, DMARC, DKIM), gdyż istnieją jeszcze inne metody (ADSP, VBR, iprev, DNSWL). W związku z tym modyfikacja ogranicza się do tego, iż dostawcy mają wyszukiwać i stosować jeden z wybranych (najlepszych) mechanizmów potwierdzania wiarygodności prawdziwości podanego nadawcy mejla.  Natomiast obie redakcje budzą trzy wątpliwości.  Po pierwsze dlaczego pomija się mniejszych dostawców usług poczty elektronicznej oraz dostawców zagranicznych, często szczególnie nadużywających, nawet w celach przestępczych komunikacji elektronicznej. Wydaje się, że konieczne jest określenie możliwych do realizacji sankcji wobec takich przypadków.  Po drugie nie jest jasna intencja twórców propozycji jakie warunki 1), 2), 3) ma spełnić dostawca – czy łącznie 1) i 2) lub 3), czy dowolny z tych trzech? Jeśli łącznie 1) i 2), to bardziej klarownym byłoby połączenie 1) i 2). Aczkolwiek to by wyłączyło obsługę podmiotów publicznych z mniej niż 500 tys. użytkowników, co jest z pewnością wbrew intencjom autorów propozycji, gdyż prawdopodobnie w skali kraju może nie być ani jednego podmiotu publicznego z taką liczbą użytkowników. Proponujemy więc z wyliczenia usunąć spójnik „lub”, a przed dwukropkiem dodać „spełniający co najmniej jeden z poniższych warunków”.  Po trzecie brak jest uzasadnienia dla liczby 500 tysięcy użytkowników/kont. Powinno się ono znaleźć co najmniej w dokumencie OSR.  Komentarz ogólny  W odniesieniu do całej treści ustawy i w szczególności do art. 1 – projektowana regulacja nie odnosi się do innych niż ujęte w propozycji formy komunikacji elektronicznej takie jak komunikatory oraz media społecznościowe, gdzie szczególnie ostatnio silnie rośnie nadużywanie wysyłania oraz publikowania treści dezinformujących oraz wymuszających szkodliwe dla odbiorcy działania. W obecnej postaci ustawa tylko częściowo będzie spełniać rolę zwalczania nadużyć w komunikacji elektronicznej. | **Uwaga nieuwzględniona**  Wskazane w przepisie mechanizmy SPF, DKIM, DMARC są najbardziej rozpowszechnione. Przepis nie zabrania stosowania dodatkowo innych mechanizmów uwierzytelnienia. |
|  | IAB Polska | Art. 14 ust. 1-2 | **UWAGA**  Art. 14 ust. 1 projektu ustawy przewiduje, że przedsiębiorcy telekomunikacyjni będą mogli przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć telekomunikacyjnych. Wyjątkiem od zasady, którą ma być brak możliwości przetwarzania komunikatu na potrzeby zwalczania nadużyć, ma być identyfikowanie, zapobieganie i zwalczanie smishingu – w tym konkretnym przypadku projekt ustawy dopuszcza przetwarzanie również komunikatu (art. 14 ust. 2 projektu ustawy).  Zacząć należy od tego, że tak sformułowany przepis (art. 14 ust. 1 i 2) obejmuje dwa różne stany faktyczne. Pierwszy to przetwarzanie danych „własnych” przedsiębiorcy telekomunikacyjnego na potrzeby zwalczania nadużyć (bez udostępniania takich danych innym przedsiębiorcom telekomunikacyjnym). Drugi to wzajemne udostępnianie danych pomiędzy przedsiębiorcami telekomunikacyjnymi celem zwiększenia skuteczności narzędzi anty-fraudowych.  W zakresie odnoszącym się do wzajemnego udostępniania danych pomiędzy przedsiębiorcami telekomunikacyjnymi należy zauważyć, że bez możliwości wymiany informacji na temat komunikatu elektronicznego skuteczność współpracy międzyoperatorskiej na rzecz zwalczania nadużyć będzie znacznie mniejsza niż mogłaby być, gdyby takiego ograniczenia nie było. O ile wzajemne udostępnianie komunikatu ma być dopuszczalne w przypadku smishingu (wiadomości SMS), o tyle taka wymiana nie będzie możliwa w przypadku nadużyć, których nośnikiem jest np. wiadomość MMS. Przestępcy wykorzystują zarówno wiadomości SMS jak i MMS do popełniania nadużyć, a o tym, czy wiadomość SMS albo MMS jest nośnikiem nadużycia o charakterze phishingowym decyduje jej treść – bez jej przetworzenia nie ma możliwości zidentyfikowania wiadomości nadużyciowych. Jednocześnie nie ma żadnych podstaw do różnicowania zakresu dopuszczalnego przetwarzania danych w zależności od tego, czy nośnikiem nadużycia jest SMS czy MMS (albo inna forma komunikatu).  O ile wyłączenie możliwości wzajemnego udostępniania komunikatu (za wyjątkiem smishingu) ograniczy skuteczność współpracy międzyoperatorskiej i utrudni skuteczną walkę z nadużyciami w komunikacji elektronicznej, to wyłączenie możliwości przetwarzania komunikatu tam, gdzie przetwarzanie ma dotyczyć „własnych” danych przedsiębiorcy telekomunikacyjnego (tj. danych dostępnych z poziomu sieci i usług świadczonych przez przedsiębiorcę telekomunikacyjnego), w zasadzie uniemożliwi przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć, w których o nadużyciowym charakterze decyduje treść komunikatu (innych niż smishing, który nie będzie objęty wyłączeniem dotyczącym komunikatu). W praktyce oznacza to, że przedsiębiorcy telekomunikacyjni nie będą mogli podejmować działań mających na celu zwalczanie nadużyć, których nośnikiem jest np. wiadomość MMS (pamiętajmy, że wiadomości MMS nie mieszczą się, i na obecnym etapie nie powinny mieścić się, w definicji smishingu).  **PROPOZYCJA:**  W naszej ocenie wyłączenie możliwości przetwarzania i udostępniania komunikatu jest szkodliwe z perspektywy celu, jakim ma być skuteczna walka z nadużyciami, w związku z czym obecne ust. 1 i 2 w art. 14 projektu ustawy powinny zostać zastąpione przepisem o następującym brzmieniu:  *“Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.”*  Przepis w takim kształcie pozwala na przetwarzanie wszystkich informacji, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, zarówno jeśli chodzi o przetwarzanie „własnych” danych jak i o ich wzajemne udostępnianie, pozwalając na walkę z obecnie znanymi formami nadużyć, jak i z takimi nadużyciami, które dopiero pojawią się w przyszłości, bez nieuzasadnionego różnicowania zakresu dopuszczalnego przetwarzania danych od tego, jaka usługa telekomunikacyjna (SMS, MMS itd.) jest nośnikiem nadużycia. Jednocześnie zaproponowany przepis jednoznacznie przesądza, że przetwarzane i wzajemnie udostępniane mogą być tylko te dane, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, co zapobiegnie przetwarzaniu i wzajemnym udostępnianiu danych innych niż niezbędne. Przykładowo, przy takim zapisie komunikat będzie mógł być przetwarzany i wzajemnie udostępniany tylko i wyłącznie wtedy, gdy o nadużyciom charakterze decyduje treść komunikatu (phishingowe SMS oraz MMS). Jednocześnie komunikat nie będzie przetwarzany i wzajemnie udostępniany w przypadku takich nadużyć, w których treść komunikatu nie ma znaczenia dla oceny, czy ruch ma charakter nadużyciowy. | **Uwaga nieuwzględniona**  Przetwarzanie treści komunikatu może stanowić bardzo istotną ingerencję w prawo do prywatności.  Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Dodatkowo, w przypadku smishingu – jako nadużycia zdefiniowanego i szerzej opisanego w ustawie, wprowadza się regulację „wzorca wiadomości”, wraz z należytymi uprawnieniami organów (CSIRT NASK). Przetwarzanie komunikatu elektronicznego powinno być ograniczone wyłącznie do zwalczania nadużyć ściśle w ustawie określonych. |
|  | Polska Izba Komunikacji Elektronicznej | Art. 14 | **Przetwarzanie i udostępnianie informacji objętych tajemnicą telekomunikacyjną *(art. 14)***  Wprowadzenie odstępstwa od obowiązku zachowania tajemnicy telekomunikacyjnej przy przetwarzaniu i udostępnianiu danych w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej należy skrytykować o tyle, że przepisy art. 13 są w tym zakresie nieprecyzyjne.  Zdaniem Izby należy konkretnie wyszczególnić cele przetwarzania i udostępniania danych, aby wykluczyć potencjalne niepożądane wykorzystanie informacji. Ponadto, w opinii Izby należy skonstruować przepis w taki sposób, by warunkiem odstępstwa od nałożonej tajemnicy telekomunikacyjnej było wykorzystanie danych na potrzeby spełnienia konkretnych celów wskazanych w przepisie. Regulacja wprost powinna określać, że to odstępstwo możliwe jest wyłącznie przy wypełnianiu obowiązków nałożonych w drodze ustawy, w szczególności tych z art. 4 ust. 6 oraz art. 8. Poważne zastrzeżenia Izby budzi przede wszystkim ujęte w ogólnym stopniu przyzwolenie na przetwarzanie i wzajemne udostępnianie informacji.  W przypadku niedoprecyzowania tej regulacji istnieje ryzyko, że przedsiębiorcy telekomunikacyjni będą wykorzystywać dane objęte tajemnicą telekomunikacyjną dla własnej korzyści, przygotowując na ich podstawie chociażby działania marketingowe. Warto również rozważyć wprowadzenie sankcji administracyjnych (np. finansowych) za naruszenie tego przepisu, by możliwie ograniczyć ryzyko nadużycia. | **Uwaga nieuwzględniona**  Zgodnie z aktualnym brzmieniem przepisów projektu odstępstwo od tajemnicy telekomunikacyjnej dotyczy wyłącznie przetwarzania i udostępniania celem identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej. Wskazany w przepisie cel wyczerpuje znamiona wykorzystywania danych na potrzeby spełnienia konkretnego celu – zgodnie z przekazaną uwagą. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 14 ust. 1 | **Przetwarzanie komunikatu na potrzeby zwalczania nadużyć (art. 14 ust. 1 i 2 projektu ustawy).**  Art. 14 ust. 1 projektu ustawy przewiduje, że przedsiębiorcy telekomunikacyjni będą mogli przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania oraz zwalczania nadużyć telekomunikacyjnych. Wyjątkiem od zasady, którą ma być brak możliwości przetwarzania komunikatu na potrzeby zwalczania nadużyć, ma być identyfikowanie, zapobieganie i zwalczanie smishingu – w tym konkretnym przypadku projekt ustawy dopuszcza przetwarzanie również komunikatu (art. 14 ust. 2 projektu ustawy).  Zacząć należy od tego, że tak sformułowany przepis (art. 14 ust. 1 i 2) obejmuje dwa różne stany faktyczne. Pierwszy to przetwarzanie danych „własnych” przedsiębiorcy telekomunikacyjnego na potrzeby zwalczania nadużyć (bez udostępniania takich danych innym przedsiębiorcom telekomunikacyjnym). Drugi to wzajemne udostępnianie danych pomiędzy przedsiębiorcami telekomunikacyjnymi celem zwiększenia skuteczności narzędzi anty-fraudowych.  W zakresie odnoszącym się do wzajemnego udostępniania danych pomiędzy przedsiębiorcami telekomunikacyjnymi należy zauważyć, że bez możliwości wymiany informacji na temat komunikatu elektronicznego skuteczność współpracy międzyoperatorskiej na rzecz zwalczania nadużyć będzie znacznie mniejsza niż mogłaby być, gdyby takiego ograniczenia nie było. O ile wzajemne udostępnianie komunikatu ma być dopuszczalne w przypadku smishingu (wiadomości SMS), o tyle taka wymiana nie będzie możliwa w przypadku nadużyć, których nośnikiem jest np. wiadomość MMS. Przestępcy wykorzystują zarówno wiadomości SMS jak i MMS do popełniania nadużyć, a o tym, czy wiadomość SMS albo MMS jest nośnikiem nadużycia o charakterze phishingowym decyduje jej treść – bez jej przetworzenia nie ma możliwości zidentyfikowania wiadomości nadużyciowych. Jednocześnie nie ma żadnych podstaw do różnicowania zakresu dopuszczalnego przetwarzania danych w zależności od tego, czy nośnikiem nadużycia jest SMS czy MMS.  O ile wyłączenie możliwości wzajemnego udostępniania komunikatu (za wyjątkiem smishingu) ograniczy skuteczność współpracy międzyoperatorskiej i utrudni skuteczną walkę z nadużyciami w komunikacji elektronicznej, to wyłączenie możliwości przetwarzania komunikatu tam, gdzie przetwarzanie ma dotyczyć „własnych” danych przedsiębiorcy telekomunikacyjnego (tj. danych dostępnych z poziomu sieci i usług świadczonych przez przedsiębiorcę telekomunikacyjnego), w zasadzie uniemożliwi przedsiębiorcom telekomunikacyjnym zwalczanie nadużyć, w których o nadużyciowym charakterze decyduje treść komunikatu (innych niż smishing, który nie będzie objęty wyłączeniem dotyczącym komunikatu). W praktyce oznacza to, że przedsiębiorcy telekomunikacyjni nie będą mogli podejmować działań mających na celu zwalczanie nadużyć, których nośnikiem jest np. wiadomość MMS (pamiętajmy, że wiadomości MMS nie mieszczą się i nie powinny mieścić się, w definicji smishingu).  W naszej ocenie wyłączenie możliwości przetwarzania i udostępniania komunikatu jest wadliwe z perspektywy celu, jakim ma być skuteczna walka z nadużyciami, w związku z czym obecne ust. 1 i 2 w art. 14 projektu ustawy powinny zostać zastąpione przepisem o następującym brzmieniu:  *Przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą komunikacji elektronicznej, niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej.*  Przepis w takim kształcie pozwala na przetwarzanie wszystkich informacji, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, zarówno jeśli chodzi o przetwarzanie „własnych” danych jak i o ich wzajemne udostępnianie, pozwalając na walkę z obecnie znanymi formami nadużyć, jak i z takimi nadużyciami, które dopiero pojawią się w przyszłości, bez nieuzasadnionego różnicowania zakresu dopuszczalnego przetwarzania danych od tego, jaka usługa telekomunikacyjna (SMS, MMS) jest nośnikiem nadużycia. Jednocześnie zaproponowany przepis jednoznacznie przesądza, że przetwarzane i wzajemnie udostępniane mogą być tylko te dane, które są niezbędne do identyfikacji, zapobiegania oraz zwalczania nadużyć w komunikacji elektronicznej, co zapobiegnie przetwarzaniu i wzajemnym udostępnianiu danych innych niż niezbędne. Przykładowo, przy takim zapisie komunikat będzie mógł być przetwarzany i wzajemnie udostępniany tylko i wyłącznie wtedy, gdy o nadużyciom charakterze decyduje treść komunikatu (phishingowe SMS oraz MMS). Jednocześnie komunikat nie będzie przetwarzany i wzajemnie udostępniany w przypadku takich nadużyć, w których treść komunikatu nie ma znaczenia dla oceny, czy ruch ma charakter nadużyciowy.  Jeśli jednak z jakichś powodów powyższa propozycja brzmienia przepisu nie zostanie zaakceptowana przez Projektodawcę proponujemy alternatywne brzmienie art. 14 ust. 1 i 2 projektu ustawy:  *Art. 14. 1. Przedsiębiorcy telekomunikacyjni mogą przetwarzać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, niezbędne do identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej.*  *2. Przedsiębiorcy telekomunikacyjni mogą wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, niezbędne do identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej.*  Tak skonstruowany przepis, zapewni przedsiębiorcom telekomunikacyjnym możliwość przetwarzania i wzajemnego udostępniania danych w zakresie stanowiącym absolutne minimum niezbędne do skutecznego identyfikowania, zapobiegania i zwalczania nadużyć. Ponadto przedstawiona powyżej propozycja brzmienia art. 14 ust. 1 i 2 porządkuje analizowane zagadnienie, rozdzielając obszar przewarzania „własnych” danych (ust. 1) od wzajemnego udostępniania danych (ust. 2), precyzyjnie określając zakres danych, które mogą być przetwarzane w każdym z tych dwóch przypadków:   * na podstawie ust. 1 przedsiębiorca telekomunikacyjny będzie miał możliwość przetwarzania (ale nie wzajemnego udostępniania) danych (w tym komunikatu elektronicznego) niezbędnych do zwalczania wszystkich form nadużyć w komunikacji elektronicznej (SMS, MMS, w których o nadużyciowym charakterze decyduje treść komunikatu); * na podstawie ust. 2 przedsiębiorcy telekomunikacyjni będą mogli wzajemnie udostępniać informacje niezbędne do zwalczania nadużyć, za wyjątkiem komunikatu elektronicznego. | **Uwaga nieuwzględniona**  Przetwarzanie treści komunikatu może stanowić bardzo istotną ingerencję w prawo do prywatności.  Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Dodatkowo, w przypadku smishingu – jako nadużycia zdefiniowanego i szerzej opisanego w ustawie, wprowadza się regulację „wzorca wiadomości”, wraz z należytymi uprawnieniami organów (CSIRT NASK). Przetwarzanie komunikatu elektronicznego powinno być ograniczone wyłącznie do zwalczania nadużyć ściśle w ustawie określonych. |
|  | Polska Izba Informatyki i Telekomunikacji | art. 13 oraz art. 14 ust. 1 – 3 | **Dopuszczalny zakres przetwarzania danych związanych ze zwalczaniem wiadomości *smishingowych*** (art. 13 oraz art. 14 ust. 1 – 3 projektu ustawy).  Wydaje się, że zachodzi wewnętrzna sprzeczność, a co najmniej niespójność wewnętrzna, jeśli chodzi o przepisy określające zasady przetwarzania danych na potrzeby zwalczania smishingu (SMS). Co więcej, obecna konstrukcja projektowanych przepisów rodzi uzasadnione obawy o spójność przetwarzania danych telekomunikacyjnych na gruncie projektowanej ustawy z zasadami przetwarzania tych danych wynikającymi z ustawy – Prawo telekomunikacyjne.  Jeśli chodzi o spójność w ramach projektowanej ustawy to należy zwrócić uwagę, że pierwszym przepisem projektowanej ustawy, który reguluje przetwarzanie danych na potrzeby zwalczania smishingu jest art. 13 ust. 1 projektu ustawy, który przewiduje, że przedsiębiorca telekomunikacyjny jest obowiązany do rejestracji danych o usługach, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku (art. 4 ust. 6) i uprawnienia (art. 7) do blokowania wiadomości smishingowych (SMS), tak, aby przedsiębiorca telekomunikacyjny był w stanie wywiązać się z obowiązku rozpatrzenia reklamacji, która w takim przypadku może być wniesiona przez abonenta. Jednocześnie art. 13 ust. 2 określa czas, przez jaki przedsiębiorca telekomunikacyjny ma przechowywać te dane (co najmniej przez okres 12 miesięcy, a w przypadku wniesienia reklamacji – przez okres niezbędny do rozstrzygnięcia sporu). Jak widać więc art. 13 ust. 1 i 2 określają zasady przetwarzania danych związanych z blokowaniem smishingowych wiadomości SMS. Okazuje się jednak, że również art. 14 ust. 3 projektu ustawy określa zasady przetwarzania danych związanych ze zwalczaniem smishingowych wiadomości SMS, ale w sposób odmienny od art. 13, gdyż w art. 14 ust. 3 wskazany jest enumeratywnie katalog przepisów projektu ustawy, których realizacja legalizuje przetwarzanie tych danych (wskazane są art. 3 ust. 2, art. 4 ust. 6, art. 7, art. 8 a także na cele związane z dochodzeniem roszczeń – taka redakcja przepisów zmusza do uznania, że przetwarzanie będzie legalne tylko w tych przypadkach). Art. 13 dotyczy przetwarzania informacji o niewykonanych usługach w związku ze zwalczaniem smishingu, a art. 14 ust. 3 dotyczy przetwarzania treści smishingowych wiadomości SMS (ust. 3 pkt 1)) oraz danych o niewykonanych usługach (ust. 3 pkt 2), pokrywając się w tym zakresie z art. 13 ust. 1). Sytuację dodatkowo komplikuje fakt, że art. 14 ust. 1 i 2 projektu ustawy (czytane razem) pozwalają na przetwarzanie wszystkich niezbędnych danych, w tym danych objętych tajemnicą telekomunikacyjną, na potrzeby identyfikowania, zapobiegania i zwalczania smishingu. I choć sama regulacja zawarta w art. 14 ust. 1 i 2 jest bardzo potrzebna, to oczywistym staje się, że regulacje zawarte w art. 13 oraz art. 14 ust. 1 – 3 są wewnętrznie niespójne, przynajmniej jeśli chodzi o zwalczanie smishingu, gdyż każdy z tych przepisów dotyczy zwalczania smisningu, ale zakres dopuszczalnego przetwarzania danych wyznacza odmiennie.  Ponadto projektowana ustawa w zakresie dotyczącym przetwarzania danych powinna być tak skonstruowana, aby uniknąć konfliktu z ustawą – Prawo telekomunikacyjne, która kompleksowo reguluje zasady i zakres przetwarzania danych telekomunikacyjnych. Przykładowo, art. 14 ust. 3 projektowanej ustawy, wskazujący enumeratywnie na przypadki, w których dane mogą być przetwarzane, budzi wątpliwości co do spójności z ustawą – Prawo telekomunikacyjne, gdyż – jedynie przykładowo – wydaje się włączać możliwość przetwarzania wiadomości SMS choćby na potrzeby wywiązania się przez przedsiębiorców telekomunikacyjnych z obowiązków zapewnienia dostępu i utrwalania na rzecz uprawnionych podmiotów, sądu lub prokuratora (art. 179 ustawy – Prawo telekomunikacyjne).  Biorąc pod uwagę, że ustawa - Prawo telekomunikacyjne kompleksowo reguluje zasady przetwarzania danych stanowiących tajemnicę telekomunikacyjną, a RODO kompleksowo reguluje przetwarzanie danych osobowych, znacznie lepszym rozwiązaniem byłoby posłużenie się w projektowanej ustawie odesłaniem do ustawy – Prawo telekomunikacyjne oraz RODO, tak, aby zasadą było, że dane stanowiące tajemnicę telekomunikacyjną są przetwarzane na zasadach określonych w ustawie – Prawo telekomunikacyjne, a dane osobowe na zasadach określonych w RODO. W projektowanej ustawie należy natomiast uwzględnić jedynie te przepisy dotyczące przetwarzania danych, które będą stanowiły *lex specialis* wobec ogólnych zasad wynikających z Prawa telekomunikacyjnego oraz RODO – przykładem takich przepisów szczególnych powinny być projektowany art. 14 ust. 1 i 2 (jako *lex specialis* wobec ustawy - Prawo telekomunikacyjne) oraz projektowany art. 14 ust. 4 (jako wyjątek od RODO). W tym celu należy stworzyć odpowiednie przepisy odsyłające do Prawa telekomunikacyjnego i RODO oraz usunąć z projektu ustawy te przepisy, które w sposób nieuzasadniony i niespójny z ustawą – Prawo telekomunikacyjne ograniczają zakres dopuszczalnego przetwarzania danych. | **Uwaga nieuwzględniona**  Art. 13 projektowanej ustawy wskazuje cele przechowywania związane z danymi o niewykonanych usługach telekomunikacyjnych w ramach prowadzenia rejestru. Wskazano, iż przechowywanie danych następuje w zakresie umożliwiającym rozpatrzenie reklamacji. Art. 14 projektowanej ustawy wskazuje w szerszym zakresie niż art. 13 dane możliwe do przetwarzania (nie tylko przechowywania), których przetwarzanie konieczne jest również do zrealizowania obowiązków wynikających z ustawy. Tym samym obejmuje ona zarówno – komplementarnie z art. 13 –przetwarzanie danych celem dochodzenia roszczeń, jak i realizację obowiązków przez przedsiębiorców związanych z walką z nadużyciami w komunikacji elektronicznej. Celem rejestru nie jest zaś realizacja obowiązków związanych z walką z nadużyciami, zaś przechowanie danych koniecznych do ewentualnego rozpatrzenia reklamacji, rozliczalności.  Przepis jest zgodny z przepisami ustawy Prawo telekomunikacyjne, wyrażonymi w art. 165 i 168, jak również z projektowanymi przepisami ustawy Prawo komunikacji elektronicznej (art. 386 ust. 2).  Projektowana ustawa stanowi *lex specialis* względem ustawy - Prawo telekomunikacyjne, opierając się jednak na przepisach z niej wynikających, w tym określających okres retencji danych, jak i prawo dostępu służb do określonych danych. |
|  | Związek Banków Polskich | Art. 14 ust. 1 - 2 | Art. 14. 1. Przedsiębiorcy telekomunikacyjni **oraz podmioty, o których mowa** **w art. 106d ust. 1 i 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)** mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą telekomunikacyjną, z wyłączeniem komunikatu elektronicznego, w celu identyfikacji, zapobiegania i zwalczania nadużyć w komunikacji elektronicznej, z uwzględnieniem ust. 2.  2. Przedsiębiorcy telekomunikacyjni **oraz podmioty, o których mowa w art. 106d ust. 1 i 1a ustawy z dnia 29 sierpnia 1997 r. – Prawo Bankowe (Dz.U. 2022 r. poz. 872, z późn. zm.)** mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu.  W związku z ewoluującymi zagrożeniami oraz coraz bardziej rozwiniętymi formami przestępczości zorganizowanej, coraz większe znaczenie ma zapewnienie efektywnej, międzysektorowej wymiany informacji prawnie chronionych.  Proponujemy zatem rozszerzenie katalogu podmiotów uprawnionych do wymiany informacji, w tym informacji objętych tajemnicą telekomunikacyjną o podmioty, które na gruncie ustawy – Prawo Bankowe uprawnione są do przetwarzania informacji objętych tajemnicą bankową w razie wystąpienia określonych przesłanek przewidzianych w rt.. 106d ust. 1 pkt 1-3 ww. ustawy.  Takie rozwiązanie umożliwiłoby wielostronną wymianę informacji w celu zapobiegania przestępstwom (uwzględniającą przedstawicieli sektora przedsiębiorców telekomunikacyjnych).  Monetyzacja nadużyć w komunikacji elektronicznej odbywa się z wykorzystaniem elektronicznych usług finansowych co tworzy konieczność integrowania działań sektora finansowego i sektora telekomunikacyjnego, w tym poprzez stworzenie warunków prawnych do wymiany informacji z wykorzystaniem centrum wymiany i analizy informacji  Przepis ten koresponduje również z propozycją stosownych zmian w treści ustawy - Prawo Bankowe. | **Uwaga nieuwzględniona w związku z nieuwzględnieniem zmian w Prawie bankowym** |
|  | IAB Polska | Art. 14 ust. 4 | **UWAGA:**  Artykuł 23 ust. 1 RODO pozwala krajowym prawodawcom wprowadzić przepisy służące ograniczeniu administratorom danych lub podmiotów przetwarzających zakresu obowiązków i praw przewidzianych w art. 12-22 RODO i w art. 34 RODO, a także w art. 5 RODO pod warunkiem, że:   1. takie przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 RODO 2. ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym i służy realizacji celów, które zostały enumeratywnie wymienione w art. 23 ust. 1 pkt a-j RODO.   IAB Polska stoi na stanowisku, że proponowane w projekcie UZNKE wyłączenie stosowania art. 14 i art. 15 RODO w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego jest konieczne, aby podmioty te mogły skutecznie przeciwdziałać przestępstwom popełnianym na ich szkodę.  Niemniej jednak przepis w obecnym kształcie znajdzie zastosowanie tylko w tych przypadkach, w których doszło do przestępstwa na szkodę przedsiębiorcy telekomunikacyjnego. Takie zawężenie może spowodować, że będzie to przepis martwy, gdyż w systemie, w którym obowiązuje domniemanie niewinności od popełnienia przestępstwa do stwierdzenie w sposób prawomocny, że przestępstwo zostało popełnione mija zazwyczaj wiele miesięcy albo i lat. Walka z nadużyciami wymaga podejmowania działań natychmiastowych.  **PROPOZYCJA:**  Biorąc powyższe pod uwagę proponujemy następującą zmianę brzmienia art. 14 ust. 4 projektu ustawy:  *Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania ~~przestępstw na szkodę przedsiębiorcy telekomunikacyjnego~~ nadużyć w komunikacji elektronicznej.* | **Uwaga uwzględniona w zakresie odwołania do nadużyć w komunikacji elektronicznej** Przepis zostanie zmieniony zgodnie z propozycją.  **Uwaga uwzględniona**  Proponuje się zmianę zapisu na nadużycia, wraz z odpowiednim rozbudowaniem opisu artykułu w uzasadnieniu projektu ustawy, uwzględniając przy tym art. 23 RODO. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 14 ust. 4 | **Relacja projektowanej ustawy do RODO (art. 14 ust. 4 projektu ustawy**)  Projekt ustawy w art. 14 ust. 4 zawiera potrzebny przepis, który w sposób precyzyjny wskazuje, które przepisy RODO nie będą stosowane w zakresie, w jakim jest to niezbędne do identyfikowania i zwalczania nadużyć. Niemniej jednak przepis ten, w obecnym kształcie znajdzie zastosowanie tylko w tych przypadkach, w których doszło do przestępstwa na szkodę przedsiębiorcy telekomunikacyjnego. Takie zawężenie może spowodować, że będzie to przepis martwy, gdyż w systemie, w którym obowiązuje domniemanie niewinności od popełnienia przestępstwa do stwierdzenie w sposób prawomocny, że przestępstwo zostało popełnione mija zazwyczaj wiele miesięcy albo i lat. Walka z nadużyciami wymaga podejmowania działań natychmiastowych. Biorąc powyższe pod uwagę proponujemy następującą zmianę brzmienia art. 14 ust. 4 projektu ustawy:  *Do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych, przepisu art. 14 i 15 rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1, z późn. zm.) nie stosuje się w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania ~~przestępstw na szkodę przedsiębiorcy telekomunikacyjnego~~ nadużyć w komunikacji elektronicznej.* | **Uwaga uwzględniona**  Proponuje się zmianę zapisu na nadużycia, wraz z odpowiednim rozbudowaniem opisu artykułu w uzasadnieniu projektu ustawy, uwzględniając przy tym art. 23 RODO. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 14 | Przechowywanie danych dot. smishingu  W art. 14 projektu wprowadza się zasady przetwarzania i wzajemnego przekazywania zastrzeżonych danych, w tym stanowiących tajemnicę telekomunikacyjną w zakresie identyfikacji, zapobiegania i zwalczania smishingu. Izba wskazuje, że przepis ten powinien wprowadzić regulacje zapobiegające wykorzystywaniu tych danych do celów innych niż związane z smishingiem. Co więcej, należy dokładnie zdefiniować na czym ma polegać zapobieganie smishingowi i czym się ono się różni od identyfikacji tego nadużycia i jego zwalczania. Zdaniem Izby obecny zapis związany z celem „zapobiegania smishingu” może prowadzić do nadużyć ze strony MNO polegających na kontroli legalnych SMS pod pozorem zapobiegania smishingowi.  Generalnie należy zwrócić uwagę, że uprawnienie z art. 14 ust. 1 i 2 projektu ustawy jest zbyt szerokie. Możliwość udostępniania komunikatów elektronicznych między przedsiębiorcami telekomunikacyjnymi jest nadmierna i powoduje, iż prywatne komunikaty użytkowników przestaną być poufne. Zapis może naruszać art. 49 Konstytucji RP, gwarantującej ochronę tajemnicy komunikowania się.  Poważne zastrzeżenia Izby budzi regulacja art. 14 ust. 3 w zakresie przechowywania danych o SMS oraz o usługach, które nie zostały świadczone w związku ze zwalczaniem smishingu. Nie jest jasne o jaki zakres danych związanych z usługami SMS tutaj chodzi. Czy chodzi tu o dane z nadawcą oraz dane niedoszłych odbiorców? Izba wyjaśnia, że przy smishingu będą to dane dziesiątków tysięcy abonentów. Wątpliwości Izby budzi kwestia przechowywanie również treści zablokowanych SMS na cele związane z roszczeniami. Czy celem tej regulacji było, aby abonenci mogli w procesie reklamacyjnym otrzymywać treść SMS, których byli nadawcami, czy też których mieli być odbiorcami? W obu przypadkach Izba nie widzi powodu do przechowywania treści zablokowanego SMS (nadawca sam go posiada). Czy przechowaniu ma podlegać jeden SMS o danej treści czy wszystkie jego kopie jakie były wysyłane do tysięcy abonentów?  Nie jest również zrozumiały zakres czasowy przez jaki przedsiębiorcy muszą przechowywać te dane. Czy chodzi tu o konieczność przechowywania wszystkich danych z art. 14 ust. 3 przez okres co najmniej 12 miesięcy? Izba zwraca uwagę, że jest to znaczące obciążenie dla przedsiębiorców telekomunikacyjnych, którzy dotychczas nie przechowywali (i nie mogli przechowywać bez zgody abonentów) blokowanych przez siebie SMS ze smishingiem. W opinii izby okres przechowywania danych o zablokowanych usługach powinien być nie dłuższy niż 30 dni, a jedynie wydłużony dla tych przypadków, w których złożono reklamację w tym czasie. 10  Ponadto Izba proponuje wprowadzenie zapisów związanych z karami za przetwarzanie i wzajemne przekazywanie danych (w tym tajemnicy telekomunikacyjnej) w celach niezwiązanych z identyfikacją i zwalczaniem smishingu.  *„art. 15 ust. 2a. Na przedsiębiorcę telekomunikacyjnego, który przetwarza lub przekazuje dane, o których mowa w art. 14 ust. 1, 2 i 3 w celach niezwiązanych z identyfikacją lub zwalczaniem smishingu może zostać nałożona kara pieniężna”.*  Dodatkowo Izba wskazuje, że przepisy RODO nie przewidują delegacji, aby pojedyncze ustawy krajowe mogły wyłączyć stosowanie art. 14 i 15 RODO.  Ograniczenie informowania na gruncie art. 14 RODO jest przewidziane w art. 14 ust. 5 RODO. Jeśli żadna z sytuacji opisanych w tym przepisie nie zachodzi, to wówczas przedsiębiorca telekomunikacyjny ma obowiązek poinformować osobę, że przetwarza jej dane. Wyjątkiem są sytuacje opisane w art. 4 oraz 5 ustawy o ochronie danych osobowych.  Przepisy RODO nie przewidują delegacji, aby można było ograniczyć stosowanie art. 14 i 15 RODO w odniesieniu do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego. | **Uwaga częściowo uwzględniona**  Doprecyzowane zostanie uzasadnienie w zakresie przetwarzania danych.  Równocześnie należy zauważyć, że Dyrektywa o prywatności 2002/58/UE w art. 5 ustanawia zasadę poufności komunikacji. Przepis zakazuje w szczególności słuchania, nagrywania, przechowywania lub innych rodzajów przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników. Wyjątkiem jest tu techniczne przechowywanie, przechowywanie celem zachowania dowodów transakcji handlowej czy inne przypadku wynikające z prawa UE lub krajowego. Przepisy prawa zawierające wyjątki od zasady poufności komunikacji powinny czynić zadość wymogom z art. 15 dyrektywy, tj. powinny stanowić środki niezbędne, właściwe i proporcjonalne w ramach społeczeństwa demokratycznego do zapewnienia bezpieczeństwa narodowego, obronności, bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektroniczne. O ile zatem w przypadku zapobiegania smishingowi, gdzie o kwalifikacji SMS-a jako nadużycia decyduje jego treść, przetwarzanie komunikatu może zostać uznane za uzasadnione i proporcjonalne do celu jakim jest ochrona przed nadużyciami, o tyle w przypadku innych rodzajów nadużyć takiego brak takiego uzasadnienia. Przetwarzanie komunikatu musi być konieczne do zidentyfikowania danego zachowania jako nadużycia. Obecne przepisy w odpowiedni sposób kształtują podstawę prawną do przetwarzania wiadomości. Jednym z obowiązków przedsiębiorców komunikacji elektronicznej będzie przeciwdziałanie smishingowi. W związku z powyższym, dla zapewnienia realnej możliwości wypełnienia tego obowiązku, konieczne jest zawarcie w przepisach podstawy prawnej dla przetwarzania danych na potrzeby jego realizacji.  Zawarty w przepisach okres przechowywania danych ma stanowić gwarancję dla użytkowników pozwalająca im dochodzić swoich praw w przypadku zablokowania ich wiadomości.  W ocenie projektodawcy nie jest konieczne uzupełnienie ustawy o dodatkowe przepisy karne.  Doprecyzowano również w przepisach kwestię stosowania RODO: „Administrator danych osobowych może wykonać obowiązek, o którym mowa w art. 13 ust. 1 i 2 oraz art. 14 ust. 1 i 2 rozporządzenia 2016/679, przez udostępnienie informacji, o których mowa w tych przepisach, na swojej stronie internetowej lub przez umieszczenie stosownych informacji w miejscach widocznych w siedzibie lub miejscu działania administratora danych osobowych.". |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 15 | Kary finansowe  Izba zwraca uwagę, że zawarte w art. 15 i kary pozbawienia wolności z art. 16 projektu ustawy mają być stosowane równolegle za to samo działanie przed dwie różne instytucje (Prezesa UKE i sąd), co wg izby jest nieprawidłową regulacją. Ponadto sankcje finansowe, z uwagi na ich dolegliwy charakter i potencjalnie dużą wysokość, wymagają poważnego doprecyzowania.  Wyjaśnienia w projekcie ustawy wymaga kwestia odpowiedzialności finansowej podmiotów zagranicznych inicjujących lub biorących aktywnie udział w nadużyciach telekomunikacyjnych. Wg wiedzy Izby większość nadużyć w komunikacji elektronicznej jest wprowadzana do polskich sieci telekomunikacyjnych z zagranicy. Zdaniem Izby, projekt powinien przewidywać regulacje związane z karaniem podmiotów zagranicznych, które są głównym źródłem nadużyć w polskich sieciach telekomunikacyjnych.  Kwestie kar finansowych powinny ulec doprecyzowaniu, za jakie konkretne czynności podlega karze finansowej przedsiębiorca telekomunikacyjny lub podmiot biorący udział w przekazywaniu komunikatów elektronicznych. Wskazujemy, że podmioty te oraz przedsiębiorcy telekomunikacyjni nie są inicjatorami smishingu czy spoofingu a jedynie wbrew ich woli ich sieci lub urządzenia są wykorzystywane do tego procederu,. Z tego względu kary finansowe powinny być związane z konkretnymi uchybieniami w zakresie zabezpieczania sieci lub urządzeń czy braku stosowania minimalnych środków zapobiegawczych. Przykładowo wskazujemy, że nie powinien być karany przedsiębiorca telekomunikacyjny, za przesłanie SMS zgodnych ze wzorcem (ale nie będących smishingiem), gdyż wg jego wiedzy pochodziły one z legalnego źródła (np. firmy kurierskiej będącej jego klientem). Nie powinno się również wprowadzać kary finansowej za niewykonanie obowiązku blokowania spoofingu, gdyż powodem takiego zaniechaniu w większości przypadków będzie brak środków technicznych do identyfikacji spoofingu. Karze finansowej powinno podlegać zaniechanie zwalczania spoofingu a nie nieskuteczne jego zwalczanie. | **Uwaga wyjaśniona**  Administracyjne kary pieniężnych będą miały charakter fakultatywny. Ponadto nawet po wszczęciu postępowania będą mogły znaleźć zastosowanie przesłanki odstąpienia od ukarania określone w art. 189e i 189f KPA. Przepisy wyraźnie wskazują, które obowiązki przedsiębiorców za powiązane z odpowiedzialnością karną. |
|  | Unia Metropolii Polskich | Art. 15 ust. 5 | Przepisy powinny w tym zakresie dawać możliwość skutecznej realizacji tego obowiązku z uwagi poprzez rozwiazywanie umów, wygaśniecie umów itp. odpowiednie vacatio legis itp. | **Uwaga wyjaśniona**  Zawarte w ustawie *vacatio legis* oraz przepisy przejściowe kompleksowo regulują tę sytuację. |
|  | Unia Metropolii Polskich | Art. 15 ust. 5 | Nie nie jest zasadne nakładanie kary w przypadku braku określenia, chociażby szacunkowych skutków finansowych wykonania tych obowiązków. | **Uwaga wyjaśniona**  Należy zauważyć, że zaproponowane rozwiązania nie są związane z istotnymi kosztami i nie powinny wymagać zatrudniania dodatkowych osób do ich skutecznego wprowadzenia. |
|  | Unia Metropolii Polskich | Art. 15 ust. 5 | Nawet jeżeli przepis o karze zostanie pozostawiony – co w naszej ocenie nie jest zasadne - to nie ma uzasadnienia aby każe podlegał kierownik podmiotu. Kara powinna zostać nałożona na podmiot, dlatego też, że obowiązek jest nałożony na podmiot tak jak większość przepisów związanych z bezpieczeństwem. | **Uwaga nieuwzględniona**  Nałożenie kary na podmiot publiczny finansowany z budżetu państwa nie będzie prowadziła do realizacji celów ustawy. Kara musi wywołać realną dolegliwość aby realizować swój cel w zakresie prewencji. Z tego względu, w przypadku podmiotów publicznych musi być nakładana na kierownika jednostki. Nałożenie kary na jednostkę prowadziłoby tylko do przesuwania środków publicznych z jednego miejsca w inne. |
|  | Unia Metropolii Polskich | Art. 15 ust. 5 | Ew. należy w uzasadnieniu wskazać, czy do stosowania kar stosuje się przepisy o kpa ?. | **Uwaga Wyjaśniona**  W zakresie kar stosowane będą przepisy niniejszej ustawy w zw. z odpowiednimi przepisami KPA. |
|  | Krajowa Izba Komunikacji Ethernetowej | Art. 16 | Kary pozbawienia wolności  Zdaniem Izby należy wskazywać, że sankcjom karnym podlegają wyłącznie podmioty, które świadomie inicjują lub wspierają określone nielegalne działania. Obecny zapis jest nieprecyzyjny, gdyż nie wskazuje, jaki podmiot podlega sankcjom karnym i za jakie konkretnie działania. Przykładowo, nie powinien podlegać sankcjom karnym przedsiębiorca telekomunikacyjny czy integrator SMS, jeśli nie brał on udział świadomie w wykorzystywaniu jego sieci lub urządzeń przez oszusta (pomocnictwo). Kwestia braku odpowiednich zabezpieczeń powinna być wyłączenie domeną kar finansowych, a nie karnych. Podmiotem podlegającym sankcjom karnym powinien być wyłącznie sam oszust, a przedsiębiorca telekomunikacyjny wyłącznie w sytuacji, gdy świadomie aktywnie brał udział w oszustwie czerpiąc z tego korzyści finansowe.  Uszczegółowieniu podlegać powinna również definicja samych zakazanych nadużyć, gdyż obecna regulacja oprócz nieprecyzyjnego technicznego ich opisu zawiera również nieprecyzyjny opis motywacji oszusta (np. spowodowania nieświadomego/niekorzystnego rozporządzania majątkiem przez ofiarę). Izba wskazuje, że przedmiot gospodarczy za pomocą którego sieci/urządzeń dokonano oszustwa (np. wyłudzono dane bankowe) nie zna motywów działania oszusta. Tymczasem definicje nadużyć telekomunikacyjnych opierają się nie tylko na aspektach technicznych, ale również na motywach sprawcy, którym nie jest przedsiębiorca telekomunikacyjny. Przykładowo projekt ustawy uzależnia nielegalność posłużenia się cudzą informacją adresową od celu w jakim to oszust zrobił (np. instalacji oprogramowania). Przedsiębiorca telekomunikacyjny nie może znać celu rozmowy telefonicznej czy wysłanego SMS. Przedsiębiorca zna jedynie motywy własnego działania lub zaniechania i tylko z tym powinna być związana jego obowiązywalność i obowiązki. Z tego względu ewentualna odpowiedzialności przedsiębiorców telekomunikacyjnych czy integratorów SMS powinna być związana wyłącznie z technicznymi aspektami działalności oszustów a nie ich motywacją.. Kwestia motywacji/ celu nadużycia telekomunikacyjnego powinna być wyłącznie wskazana w przepisach karnych.  Generalnie izba również wskazuje, że proponowane kary pozbawienia wolności są odmienne niż obecnie w kodeksie karnym. Przykładowo generowanie sztucznego ruchu z art. 3 ust. 1 pkt 1 projektu może pokrywać się zakresem z kradzieżą impulsów telekomunikacyjnych z art. 285 kk a jednocześnie jest zagrożone wyższą karą. Oszustwo z kolei w kk jest zagrożone karą wyższą, mimo że oszustwo przy użyciu smishingu może mieć charakter masowy, a więc poważniejszy. Zdaniem izby, przepisy karne o nadużyciach (ale nie o karach finansowych) dublują obecne regulacje z kodeksu karnego (np. w zakresie oszustwa, jakim jest bez wątpienia spoofing).  Izba ponownie zwraca uwagę na brak wyjaśnienia jaka jest równica między nadawaniem widomości SMS a inicjowaniem ich wysyłania (a także jaka jest równica między samym nadawaniem a wysyłaniem – oba zwrot wydają się być stosowane w projekcie zamiennie). Nakładanie kar z tytułu dopuszczania się działań, które są nie tylko niezdefiniowane, ale i niemające jednoznacznego powszechnego znaczenia jest niedopuszczalne. | **Uwaga uwzględniona w zakresie ujednolicenia stosowania pojęć „nadawaniem widomości SMS” a „inicjowania ich wysyłania”**  **Uwaga nieuwzględniona w pozostałym zakresie**  Zgodnie z ogólnymi zasadami prawa karnego założeniem jest umyślne działanie sprawców tych przestępstw. Nie istnieje więc możliwość ukarania za te czyny nieświadomego ich przedsiębiorcy telekomunikacyjnego.  Wykorzystane w przepisach karnych sformułowania w wystarczający sposób określają znamiona czynów zabronionych. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 15  Art. 16 | **Kary**  Jak już wcześniej zostało podniesione kluczowe jest, aby ryzyko kary ciążyło na sprawcach dopuszczających się nadużyć w komunikacji elektronicznej i tą funkcję mają realizować art. 15 ust. 1 oraz art. 16 projektu ustawy. Jednocześnie projektowana ustawa jako zasadę powinna przewidywać uprawnienie dla przedsiębiorców telekomunikacyjnych do zwalczania nadużyć w komunikacji elektronicznej, a działanie w reżimie obowiązku można sobie wyobrazić jako wyjątek od zasady (jaką powinno być uprawienie) tylko dla blokowania SMS wpisujących się we wzorzec przekazany przez NASK (art. 4 ust. 6 projektu ustawy) oraz połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego do wykazu numerów służących wyłącznie do odbierania połączeń głosowych, prowadzonego przez Prezesa UKE (art. 9 ust. 12 projektu ustawy). Nie jest konieczne wprowadzanie ryzyka kar pieniężnych za niewywiązanie się z obowiązku blokowania SMS albo połączeń inicjowanych z wykorzystaniem numeru wpisanego do wykazu, jeśli jednak w ocenie Projektodawcy takie kary są niezbędne, to powinny one dotyczyć tylko tych dwóch obowiązków i powinny mieć charakter fakultatywny.  Jeśli zwalczanie CLI spoofingu ma się obywać w reżimie obowiązku (art. 8 projektu ustawy) pod groźbą kary pieniężnej ze strony Prezesa UKE (art. 15 ust. 2 pkt 2) projektu ustawy) to konieczne będzie wyznaczenie organu państwa, który będzie identyfikował konkretne połączenia głosowe jako CLI spoofing i przekazywał taką informację przedsiębiorcom telekomunikacyjnym celem zablokowania tak zidentyfikowanych połączeń (analogicznie do zaprojektowanego mechanizmu identyfikowania smishingowych wiadomości SMS przez NASK). Tak zidentyfikowane przez organ państwa połączenia głosowe przedsiębiorcy telekomunikacyjni mogą blokować w reżimie obowiązku.  Jeśli jednak nie jest możliwe wyznaczenie organu państwa odpowiedzialnego za identyfikowanie spoofowanych połączeń głosowych, to:   * projekt ustawy należy przeredagować tak, aby obowiązek w tym zakresie (art. 8 projektu ustawy) zmieć w uprawnienie:   *Art. 8. W przypadku uzasadnionego podejrzenia wystąpienia CLI spoofingu przedsiębiorca telekomunikacyjny może zablokować takie połączenie albo wyeliminować prezentację identyfikacji numeru wywołującego.*   * należy usunąć z projektu ustawy ryzyko kary przewidziane w art. 15 ust. 2 pkt 2).   Przedsiębiorcy telekomunikacyjni budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów (CLI spoofing). Takie rozwiązania i mechanizmy zapobiegające nadużyciom musimy próbować tworzyć sami, na gruncie współpracy międzyoperatorskiej i w porozumieniu z pozostałymi krajowymi operatorami. Tym celom ma służyć mechanizm, który zgodnie z art. 10 projektu ustawy ma działać w oparciu o porozumienie z Prezesem UKE. Prawidłowe realizowanie porozumienia ma oznaczać prawidłowe wykonywanie obowiązku wynikającego z art. 8 (tak wynika, i słusznie, z art. 10 ust. 2 i 3 projektu ustawy), jednak nie każdy przedsiębiorca telekomunikacyjny będzie dysponował zasobami i wiedzą niezbędną do przystąpienia i realizacji porozumienia. Obowiązek oraz ryzyko kary za nieskuteczne zwalczanie CLI spoofingu (art. 8 w zw. z art. 15 ust. 2 pkt 2) projektu ustawy) z jednej strony i możliwość skorzystania z ochrony oferowanej przez przystąpienie i realizowanie porozumienia (art. 10 ust. 2 i 3 projektu ustawy) z drugiej strony może spowodować, że znaczna część z kilku tysięcy przedsiębiorców telekomunikacyjnych działających w Polsce będzie chciała przystąpić do porozumienia, tylko po to, aby zminimalizować ryzyko kar, choć znaczna część z tych przedsiębiorców, nie mając własnych sieci telekomunikacyjnych, niezbędnej wiedzy i zasobów, nie będzie w stanie realizować wymagań technicznych. W efekcie może się okazać, że zawarcie i realizowanie porozumienia zostanie sparaliżowane przez wnioski o akces do porozumienia ze strony licznych przedsiębiorców telekomunikacyjnych nieposiadających własnych sieci telekomunikacyjnych, tylko po to, aby zminimalizować ryzyko kary. Ryzyko kary w tym przypadku może sprawić, że porozumienie przestanie być zarządzalne w krótkim czasie po jej uruchomieniu.  W zakresie zwalczania CLI spoofingu w zupełności wystarczające jest ryzyko kary dla przedsiębiorcy telekomunikacyjnego, który nie wypełni obowiązku blokowania połączeń głosowych inicjowanych z wykorzystaniem numeru wpisanego na listę numerów służących wyłączenie do odbierania połączeń (art. 15 ust. 2 pkt 3) projektu ustawy – aczkolwiek również to ryzyko powinno być usunięte, patrz wcześniejsze uwagi). Bardziej zaawansowane technologicznie rozwiązania, w tym rozwiązania nowatorskie i wręcz eksperymentalne, powinny działać w ramach porozumienia, a samo porozumienie powinno być:   * otwarte na akces operatora gotowego przyjąć na siebie ciężar realizacji porozumienia; * a jednocześnie dobrowolne dla każdego operatora, a nie pośrednio wymuszane reżimem obowiązku i widmem kary pieniężnej. | **Uwaga nieuwzględniona**  Kary mają zapewnić skuteczność projektowanych obowiązków. Podkreślić należy, że kary będą fakultatywne i za niewykonanie konkretnych obowiązków. Ponadto nawet po wszczęciu postępowania będą mogły znaleźć zastosowanie przesłanki odstąpienia od ukarania określone w art. 189e i 189f KPA. |
|  | Polska Izba Komunikacji Elektronicznej | Art. 15 ust. 1 i 2 | **Kara pieniężna za nadużycia w komunikacji elektronicznej *(art. 15 ust. 1 i 2)***  Przepis przewidujący nałożenie sankcji administracyjnej na podmioty dokonujące nadużyć (ust. 1) jest w opinii Izby niepełny i wymaga dopracowania. Przede wszystkim nieprecyzyjnie wskazuje się zakres podmiotowy przepisu. Przez to nie jest wiadome kto podlega karze - czy jest to jedynie podmiot inicjujący nadużycie (np. połączenie głosowe), czy również operator, który pośredniczy w procesie nieświadomie. Postulujemy, aby przede wszystkim regulacja określała w sposób wyraźny zakres podmiotowy oraz zakres przedmiotowy swojego zastosowania, poprzez wskazanie na konkretną sytuację, w której możliwe jest nałożenie kary administracyjnej. Dopracowanie przepisu pozwoli wprost przedstawić możliwe sytuacje, w których przedsiębiorca telekomunikacyjny byłby zagrożony poniesieniem odpowiedzialności.  Podkreślić należy również, że uwagi powinno się odnieść również do ust. 2. Przepis ten zakłada możliwość nałożenia na przedsiębiorcę telekomunikacyjnego kary pieniężnej za niewypełnienie obowiązków, o których mowa w art. 4 ust. 6, art. 8, art. 9 ust. 12. Niemniej jednak, przepis ten nie wskazuje wyraźnie zakresu podmiotowego i przedmiotowego zastosowania. Na jego podstawie ponownie nie jest jasne, czy przepis dotyczy wszystkich przedsiębiorców biorących udział w procesie nadużycia (np. kilku operatorów, w których sieciach przekazywane jest to samo połączenie), czy jedynie przedsiębiorcę odpowiedzialnego za zainicjowanie działania stanowiącego nadużycie. Ta kwestia powinna być określona wprost. Jeżeli chodzi natomiast o zakres przedmiotowy, to w opinii Izby należy w tym przepisie wskazać wyraźnie, jakie działania lub zaniechania mogą stanowić podstawę do nałożenia kary pieniężnej (np. czy kary są związane wyłącznie ze świadomym działaniem, czy również z brakiem odpowiednich zabezpieczeń).  PIKE pragnie wskazać również na poważny problem związany z pominięciem w przepisie podmiotów zagranicznych i ograniczeniem go do podmiotów polskich. Problem spowodowany jest faktem, że działania stanowiące nadużycia w ogromnej części pochodzą z zagranicznych sieci. Należy rozważyć tę kwestię, ponieważ nie jest jasne, w jaki sposób takie działania powinny być traktowane w kontekście proponowanych sankcji. Na marginesie należy również wspomnieć, że kwestie związane z nadużyciami pochodzącymi z zagranicy powinno się rozważyć w odniesieniu do całej ustawy. W przeciwnym wypadku proponowane środki okażą się najprawdopodobniej niewystarczające do spełnienia swoich funkcji. Niewzięcie pod uwagę tego aspektu w ustawie podważa jej skuteczność. | **Uwaga wyjaśniona**  Obecne art. 15 w ust. 1-3 precyzuje odpowiedzialność poszczególnych podmiotów. Przedsiębiorcy telekomunikacyjni ponoszą odpowiedzialność administracyjną za niewypełnianie obowiązków określonych w:  1) art. 4 ust. 6,  2) art. 8,  3) art. 9 ust. 12  Obecne przepisy precyzują w wystarczającym stopniu znamiona czynów zabronionych określone w tym przepisie. W zakresie interpretacji tych przepisów należy zastosować ogólne zasady. |
|  | Związek Banków Polskich | Art.15 ust. 2 pkt 3 | art. 9 ust. 12 i 13  Konsekwencja wprowadzenia dodatkowego obowiązku jw. | **Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwag do art. 9** |
|  | Polska Izba Komunikacji Elektronicznej | Art. 16 | **Przepis karny *(art. 16)***  PIKE zaznacza, że art. 16, stanowiący w całości przepis karny, nie powinien w jej opinii znaleźć się w przedmiotowej regulacji. Przepis dubluje w pewnym zakresie rozwiązania już obecne w Kodeksie karnym – m.in. art. 190a § 2, art. 285, art. 286. Projektodawca powinien zatem rozważyć kwestię przeniesienia przepisu właśnie do Kodeksu karnego albo zmodyfikowania projektowanych regulacji w taki sposób, aby usuwały wątpliwości co do ich relacji do przepisów Kodeksu karnego. | **Uwaga nieuwzględniona**  Zdaniem projektodawcy kwestia przestępstw mających charakter nadużyć w komunikacji elektronicznej powinna być uwypuklona w odrębnym przepisie. |
|  | Polska Wytwórnia Papierów Wartościowych | art. 16 ust. 3 | W art. 16 ust. 3 projektu ustawy użyto wyrażenia „osoba najbliższa”. Z uwagi na brak jednoznacznego znaczenia tego wyrażenia w polskim systemie prawnym proponujemy rozważyć wprowadzenie w art. 16 ust. 3 odwołania do art. 115 § 11 kodeksu karnego lub zamieszczenie definicji pojęcia „osoba najbliższa” w art. 2 projektu ustawy. | **Uwaga wyjaśniona**  Zgodnie z art. 116 Kodeksu karnego przepisy części ogólnej tego kodeksu stosuje się do innych ustaw przewidujących odpowiedzialność karną. Dlatego nie ma potrzeby dodawania definicji osoby najbliższej w projekcie. W uzasadnieniu przepisu zostanie dodane stosowne wyjaśnienie. |
|  | Polska Wytwórnia Papierów Wartościowych | Art. 19 | Zgodnie z treścią art. 19 projektu, CSIRT NASK będzie miał obowiązek uruchomienia systemu teleinformatycznego służącego przekazywaniu informacji o wystąpieniu smishingu. Sposób działania CSIRT NASK określa przepis art. 4 projektu, który reguluje m. in. przesyłanie wiadomości do podmiotów o nadużyciach w komunikacji elektronicznej. Niemniej jednak przekazujemy do rozważenia uzupełnienie ww. regulacji i wskazanie, że CSIRT NASK zarówno uruchamia jak i utrzymuje system teleinformatyczny. | **Uwaga uwzględniona**  Zostanie wskazane, że CSIRT NASK uruchamia i utrzymuje systemie teleinformatyczny. |
|  | IAB Polska | Art. 20,  Art. 23 | **UWAGA:**  W przeciwieństwie do innych przedsiębiorców telekomunikacyjnych UZNKE **nie przewiduje okresu dostosowawczego dla dostawców poczty elektronicznej**, zatem będą oni mieli jedynie **30-dniowy okres *vacatio* *legis***, aby dostosować się do obowiązków określonych w projekcie UZNKE, co może okazać dla nich za krótkim terminem, aby przygotować się do realizacji tych obowiązków. Oznacza to ryzyko nałożenia kary pieniężnej na dostawcę poczty elektronicznej, który w tak krótkim czasie nie wywiąże się z obowiązków określonych w UZNKE.  **PROPOZYCJA:**  IAB Polska proponuje dodanie w art. 20 UZNKE nowego punktu:  *3) o której mowa w art. 15 ust. 3, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.* | **Uwaga nieuwzględniona** Wdrożenie mechanizmów SPF, DKIM oraz DMARC jest stosunkowo proste a ich wdrożenie przekroczyć maksymalnie kilku dni roboczych. |
|  | Polska Izba Informatyki i Telekomunikacji | Art. 20 | **Okres przejściowy dla kar pieniężnych**  Art. 20 projektowanej ustawy przewiduje swoistą karencję, określony czas liczony od momentu wejścia w życie ustawy, przez który Prezes UKE nie będzie nakładał na przedsiębiorców telekomunikacyjnych kar pieniężnych za niewykonanie obowiązków wynikających z projektowanej ustawy. W ocenie Izby art. 20 powinien zyskać następujące brzmienie:  *Art. 20. Kary pieniężnej:*  *1) o której mowa w art. 15 ust. 2 pkt 1, nie nakłada się przed upływem 6 miesięcy od dnia wejścia w życie ustawy;*  *2) o której mowa w art. 15 ust. 2 pkt 2 i 3, nie nakłada się przed upływem 12 miesięcy od dnia wejścia w życie ustawy.*  Obecnie w art. 20 projektowanej ustawy brakuje przepisu, który odnosiłby się do nakładania kary pieniężnej, w przypadku, o którym mowa w art. 15 ust. 2 pkt 3) projektu ustawy, czyli blokowania połączeń inicjowanych z wykorzystaniem numerów wpisanych do wykazu prowadzonego przez Prezesa UKE. W tym przypadku należy terminy skonfigurować tak, aby dać Prezesowi UKE czas na opracowanie i wdrożenie wykazu oraz czas niezbędny przedsiębiorcom telekomunikacyjnym na uruchomienie blokowania połączeń identyfikujących się numerem wpisanym do wykazu.  Jednocześnie zwracamy uwagę, że jeśli zostanie uwzględniony nasz wcześniejszy postulat dotyczący usunięcia art. 15 ust. 2 pkt 2) projektu ustawy (ryzyko kary za niewykonanie obowiązku wynikającego z art. 8) to obecny punkt 3) w ust. 2 w art. 15 zamieni się w punkt 2) i w takim przypadku nie będą konieczne żadne zmiany w art. 20 projektu ustawy. | **Uwaga nieuwzględniona**  W ocenie projektodawcy taka zmiana nie jest konieczna. Przedsiębiorca telekomunikacyjny będzie obowiązany blokować połączenia inicjowane z numerów znajdujących się w wykazie. Jeżeli wykaz będzie w fazie tworzenia, to nie będzie aktualizował się obowiązek blokowania połączeń. |
|  | Związek Banków Polskich | Propozycje zmian w ustawie z dnia 29 sierpnia 1997 r. - Prawo bankowe | Art. 4 ust. 1 pkt 59 (nowy)  **59) centrum wymiany i analiz informacji – podmiot sektora finansowego, upoważniony do przetwarzania informacji na temat podatności, zagrożeń lub incydentów, mogących lub mających wpływ na bezpieczeństwo podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów,**  **60) przedsiębiorca telekomunikacyjny – przedsiębiorca, o którym mowa w art. 2 pkt 27 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne;**  Wobec identyfikacji coraz liczniejszych podatności, zagrożeń i incydentów wpływających na bezpieczeństwo sektora finansowego i jego klientów istnieje konieczność powołania nowej kategorii instytucji, której głównym zadaniem będzie koordynowanie obsługi incydentów wymierzonych podmioty sektora finansowego i ich klientów oraz wymienianie informacji na temat podatności i zagrożeń. Powołanie centrum wymiany i analizy informacji oraz nadanie mu stosownych ustawowych uprawnień istotnie wpłynie na wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę instytucji finansowych lub ich klientów oraz wspieranie organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. W tym celu centrum wymiany i analizy informacji oraz inne podmioty wymienione w art. 106d ust. 1 i 1a powinny mieć m. in. możliwość wymienianie się informacjami prawnie chronionymi, w tym tajemnicą bankową.    Art. 106 ust. 6-8 (nowe)  **6. Bankowa izba gospodarcza, wspólnie z bankami, może utworzyć centrum wymiany i analiz informacji, upoważnione do gromadzenia, przetwarzania i udostępniania informacji, w tym informacji prawnie chronionych, w celu i zakresie, o których mowa w art. 106d oraz w odrębnych przepisach.**  **7. Do zadań centrum wymiany i analizy informacji należy, w szczególności:**  **1) wykrywanie, analizowanie i przeciwdziałanie przestępstwom popełnianym na szkodę podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów;**  **2) koordynowanie obsługi incydentów zagrażających bezpieczeństwu podmiotów, o których mowa w art. 106d ust. 1 oraz 1a lub ich klientów;**  **3) wymiana informacji, dobrych praktyk i doświadczeń dotyczących podatności, zagrożeń, obsługi incydentów oraz ich koordynacji;**  **4) wspieranie banków w wykonywaniu obowiązków, o których mowa w ust. 1.**  **8. Centrum wymiany i analizy informacji może wspierać organy ścigania w wykrywaniu i ściganiu sprawców przestępstw, o których mowa w ust. 7 pkt 1.**  Bankowa izba gospodarcza, wspólnie z bankami, powinna mieć prawną możliwość utworzenia centrum wymiany i analizy informacji, które będzie wspierać banki oraz inne instytucje rynku finansowego w zakresie identyfikacji podatności, neutralizacji zagrożeń oraz koordynacji obsługi incydentów zagrażających bezpieczeństwu instytucji finansowych lub ich klientów. Szczegółowe zadania centrum wymiany i analizy informacji zostały określone w propozycji art. 106 ust. 6-8.  Dodatkowo, centrum wymiany i analizy informacji powinno mieć możliwość wspierania organów ścigania w zakresie wykrywania i ścigania sprawców tych przestępstw. Dotychczasowe doświadczenia FinCERT.pl – BCC ZBP, Prokuratury Krajowej i Komendy Głównej Policji oraz Komend Wojewódzkich Policji pozwalają stwierdzić, że powoływane wspólnie tzw. Grupy Operacyjne pozwalają na sprawne skoordynowanie działań po stronie sektora finansowego oraz organów ścigania co wydatnie wpływa na efektywność działań podejmowanych przez wszystkich interesariuszy.  Art. 106d ust. 1-2  1. Banki, inne instytucje ustawowo upoważnione do udzielania kredytów, izby rozliczeniowe utworzone na podstawie art. 67, instytucje utworzone na mocy art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorcy telekomunikacyjni**,** mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową, w przypadkach:  1) uzasadnionych podejrzeń, o których mowa w art. 106a ust. 3;  2) uzasadnionych podejrzeń popełnienia przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim**,** przedsiębiorców telekomunikacyjnych i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom;  3) wykonywania obowiązków w zakresie określonym w przepisach o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.  2. Podmioty określone w ust. 1 mogą przetwarzać i wzajemnie udostępniać informacje, w tym informacje objęte tajemnicą bankową oraz informacje dotyczące wyroków skazujących, w przypadkach przestępstw dokonywanych na szkodę banków, innych instytucji ustawowo upoważnionych do udzielania kredytów, instytucji kredytowych, instytucji finansowych, instytucji pożyczkowych oraz podmiotów, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorców telekomunikacyjnych i ich klientów, w celu i zakresie niezbędnym do zapobiegania tym przestępstwom.  Konsekwencja wcześniej zaproponowanych zmian – uzasadnienie jw. W określonych okolicznościach, o których mowa w art. 106d ust. 1 również przedsiębiorcy telekomunikacyjni powinni mieć prawną możliwość przetwarzania informacji objętych tajemnicą bankową.  Art. 106d ust. 1a  **1a. W przypadkach określonych w ust. 1, do przetwarzania i wzajemnego udostępniania informacji, w tym objętych tajemnicą bankową, uprawnione są również następujące podmioty:**  **1) centrum wymiany i analizy informacji, o którym mowa w art. 106 ust. 6;**  **2) podmioty, które są członkami centrum wymiany i analizy informacji, o którym mowa w pkt 1 lub zawarły z nim stosowne porozumienie w zakresie, o którym mowa w ust. 1;**  Uzasadnienie jw.  Do przetwarzania danych osobowych przez banki, inne instytucje ustawowo upoważnione do udzielania kredytów oraz instytucje utworzone na podstawie art. 105 ust. 4, jednostki zarządzające systemem ochrony, o których mowa w art. 22d ust. 1 pkt 2 ustawy o funkcjonowaniu banków spółdzielczych, ich zrzeszaniu się i bankach zrzeszających, jednostki zarządzające systemem ochrony, o których mowa w art. 130e ust. 1, instytucje pożyczkowe, instytucje finansowe, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu lub świadczeniu usług faktoringowych, podmioty, których podstawowa działalność polega na udostępnianiu składników majątkowych na podstawie umowy leasingu, oraz podmioty, o których mowa w art. 59d ustawy z dnia 12 maja 2011 r. o kredycie konsumenckim, przedsiębiorców telekomunikacyjnych,przepisu art. 15 rozporządzenia 2016/679 nie stosuje się w zakresie, w jakim jest to niezbędne dla prawidłowej realizacji zadań dotyczących przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu, zgodnie z art. 106, oraz zapobiegania przestępstwom, zgodnie z art. 106a i art. 106d.  Konsekwencja wcześniej zaproponowanych zmian – uzasadnienie jw. | **Uwaga nieuwzględniona**  Regulacje dotyczące ISAC – centrum wymiany i analiz informacji znajdują się w projekcie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. |
|  | Polska Izba Informatyki i Telekomunikacji | Uzasadnienie | **Uwagi do uzasadnienia do projektu ustawy**  Akapit drugi na stronie pierwszej uzasadnienia do projektu ustawy ma następujące brzmienie (podkreślenie własne):  *W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć. Oszuści wykorzystywali w ten sposób słabości sieci telekomunikacyjnych, które powodują, że operatorzy sieci mobilnych często nie są w stanie zweryfikować, czy połączenie w ramach którego jest prezentowany numer faktycznie pochodzi z karty SIM, która jest zarejestrowana dla danego numeru. Zjawisko to występuje pod nazwą CLI spoofing.*  Proponujemy, aby ten fragment tekstu uzyskał następujące brzmienie:  *W ostatnich miesiącach nasiliły się również ataki na osoby fizyczne z wykorzystaniem usług telekomunikacyjnych. Przestępcy, stosując specjalne bramki internetowe VoIP podszywali się pod numer zaufanych instytucji czy osoby publiczne i dzwonili z rzekomo prawdziwego numeru. W ten sposób próbowali nakłonić odbiorców do niekorzystnego działania czy w niektórych przypadkach nawet próbowali ich zastraszyć.*  *Proceder CLI spoofingu polega na nieuprawnionym posłużeniu się przez użytkownika (często przestępcę) wywołującego połączenie głosowe numerem wskazującym na inną osobę lub instytucję, po to, aby podszyć się pod tą osobę albo instytucję i dzięki temu móc łatwiej nakłonić ofiarę (tj. odbiorcę takiego połączenia) do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem lub instalacji złośliwego oprogramowania.*  *Z doświadczeń krajowych operatorów wynika, że gros połączeń z numerem A wykorzystywanym przez osobę nieuprawnioną przychodzi do naszego kraju z zagranicy. Źródłem spoofingu są więc przestępcy, którzy korzystają z usług telekomunikacyjnych oferowanych przez dostawców działających w krajach o niskich standardach biznesowych i regulacyjnych. To również znacznie utrudnia organom ścigania wykrycie sprawców. W przypadku gdy połączenie ze spoofowanym numerem A przychodzi do krajowych sieci telekomunikacyjnych z zagranicy, dla krajowych operatorów takie połączenie nie różni się niczym od innych, „legalnych” połączeń. W przypadku połączeń przychodzących z zagranicznych sieci operator krajowy „widzi” numer A i numer B połączenia i na dzień dzisiejszy nie ma możliwości ustalenia w czasie rzeczywistym i bez możliwości udziału w tym procesie sieci i operatorów biorących udział w zainicjowaniu oraz pośredniczących w realizacji połączenia, czy numer A jest wykorzystywany przez osobę uprawnioną, czy przez osobę nieuprawnioną. Innymi słowy, na dzień dzisiejszy połączenie ze spoofowanym numerem A z perspektywy operatora krajowego „wygląda” dokładnie tak samo, jak połączenie, w którym numerem A posługuje się osoba uprawniona. O tym, że połączenie jest spofowane wie tylko osoba inicjująca połączenie (w momencie jego inicjowania), a w momencie odebrania połączenia albo później dowiaduje się o tym osoba odbierająca połączenie (numer B). Operator telekomunikacyjny, organy ścigania, instytucje, pod które podszył się przestępca, dowiadują się o tym, że połączenie było spoofowane, dopiero po fakcie, od ofiary (numer B), która odebrała takie połączenie. To tłumaczmy, czemu proceder CLI-spoofingu istnieje i czemu tak trudno jest go wyeliminować czy choćby ograniczyć.*  Celem zaproponowanej zmiany jest, aby opis zjawiska CLI spoofingu był bardziej adekwatny do tego, jak faktycznie działa ten mechanizm. Ponadto, nie możemy zgodzić się ze stwierdzeniem sugerującym, że to „słabości” sieci telekomunikacyjnych umożliwiają przestępcom działanie. Operatorzy budują sieci i świadczą usługi telekomunikacyjne na podstawie standardów, norm, wytycznych i zasad, które są ustalane oraz koordynowane na poziomie międzynarodowym – ITU, ETSI, 3GPP. Stosując powszechnie uznane, międzynarodowe standardy techniczne dochowujemy najwyższej możliwej staranności, zapewniając naszym klientom interoperacyjne, niezawodne i bezpieczne usługi telekomunikacyjne o zasięgu globalnym. Istniejące standardy techniczne dla sieci telekomunikacyjnych nie przewidują gotowych rozwiązań i narzędzi, które można by wykorzystać do identyfikowania połączeń telekomunikacyjnych, które są zestawiane zgodnie z przyjętymi normami technicznymi, a które są inicjowane przez przestępców dla osiągnięcia niezgodnych z prawem celów. Fakt, że przestępcy nadużywają sieci i usług telekomunikacyjnych do popełniania przestępstw w żadnym wypadku nie świadczy o jakiejkolwiek „słabości” albo wadzie sieci telekomunikacyjnych, tak jak popełnienie przestępstwa z użyciem noża nie świadczy w żaden sposób o tym, że nóż jest w jakikolwiek sposób wadliwy.  Nie można również zapominać, iż CLI-spoofing nie jest celem samym w sobie, jest narzędziem, jednym z wielu w przestępczym repertuarze, wykorzystywanym w celu zwiększenia szansy powodzenia przestępczego ataku. Zresztą przestępcy nie zawsze wykorzystują CLI-spoofing dzwoniąc do ofiary, czasami takie połączenia są realizowane z numeru zastrzeżonego albo z dowolnego innego, pokazującego się numeru (który nie został spoofowany). Najważniejszą część takiego ataku stanowi socjotechnika wykorzystywana przez przestępców do skłonienia ofiary do postępowania zgodnie z ich poleceniami. Próby ograniczenia CLI-spoofingu na poziomie sieci telekomunikacyjnych można porównać do usuwania jedynie niektórych objawów choroby, bez leczenia samej choroby. Ową chorobą w tym przypadku są przestępcy, którzy dzwonią do ofiar (wykorzystując CLI-spoofing albo nie) i podszywając się pod inną osobę, instytucję publiczną albo firmę skłaniają ofiarę do przekazania danych czy podjęcia czynności, w efekcie których ofiara traci pieniądze albo doznaje szkody w innej postaci. Oznacza to również, że nawet jeśli uda się do pewnego stopnia ograniczyć zjawisko CLI spoofingu, to nie będzie to oznaczało, że przestępcy zaprzestaną swojego przestępczego procederu, gdyż tak długo, jak proceder będzie opłacalny a sprawcy nieuchwytni i bezkarni, przestępcy będą wykonywali przestępcze połączenia albo próbując ominąć zabezpieczenia CLI spoofingowe albo dzwoniąc z dowolnego numeru zastrzeżonego albo widocznego (który nie został spoofowany) i bez CLI spofingu będą próbowali przekonać ofiarę, że są pracownikiem instytucji finansowej albo publicznej. | **Uwaga częściowo uwzględniona** Uzasadnienie zostanie uzupełnione. Usunięty został fragment o „słabości sieci” jako zbytnie uproszczenie. |

1. <https://sjp.pwn.pl/slowniki/SMS.html> [↑](#footnote-ref-2)
2. <https://sjp.pwn.pl/slowniki/SMS.html> [↑](#footnote-ref-3)
3. <https://cert.pl/posts/2020/03/ostrzezenia_phishing/> [↑](#footnote-ref-4)
4. <https://cert.pl/posts/2020/03/ostrzezenia_phishing/> [↑](#footnote-ref-5)