|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Lp. | Instytucja | Jednostka redakcyjna | Treść uwagi | Odniesienie |
|  | UKE | Uwaga ogólna | Uwaga ogólna -projektowana ustawa nakłada na UKE całkowicie nowe zadania, które wymagają wiedzy specjalistycznej, co wiąże się z koniecznością zatrudnienia albo co najmniej przeszkolenia pracowników. Niezbędne jest zatem zapewnienie środków dla Urzędu na realizację ww. zadań. | **Uwaga nieuwzględniona**  Nowe zadania są ściśle powiązane z dotychczasowymi zadaniami UKE, w związku z czym urząd posiada już niezbędne kadry. W związku z tym możliwa jest realizacja nowych zadań w ramach posiadanych środków. |
|  | UOKIK | Uwaga ogólna | Należy podkreślić, że projekt oraz zaprojektowane w nim rozwiązania należy co do zasady ocenić pozytywnie, szczególnie uwzględniając rosnącą liczbę stwierdzonych przypadków tzw. smishingu oraz spoofingu. Tego typu działania są sprzeczne z prawem i bezpośrednio prowadzą do znacznych strat finansowych po stronie konsumentów. Prezes Urzędu Ochrony Konkurencji i Konsumentów (dalej jako „Prezes UOKiK”) otrzymuje zgłoszenia od osób, które były celem tego typu ataków. Rozwiązania prowadzące do zwiększenia ochrony konsumentów przed tego typu działaniami powinno się zatem uznać za pożądane.  Jednocześnie wskazać należy, że projekt wymaga dopracowania w niektórych jego aspektach. W szczególności dotyczy to zagadnienia tzw. „sztucznego ruchu”, które zostało zdefiniowane w tekście projektowanej ustawy, jednak nie zostało w jakikolwiek sposób rozwinięte w jej treści. Sztuczny ruch został wyszczególniony w art. 3 jako nadużycie w komunikacji elektronicznej, brakuje jednak w projekcie przepisów szczegółowych, których celem byłoby przeciwdziałanie lub zwalczanie do tego typu aktywności, analogicznie do przepisów dotyczących smishingu oraz spoofingu. Projekt wyraźnie koncentruje się na wspomnianych dwóch zjawiskach.  Niezbędne jest przy tym wskazanie, że Prezes UOKiK w swojej praktyce spotkał się z przypadkami, w których wykonujący dużo połączeń konsumenci (zwykle korzystający z taryf „bez limitu”) stawali się (niezamierzonym) celem mechanizmów lub działań ze strony operatorów telekomunikacyjnych, mających na celu przeciwdziałanie sztucznemu ruchowi. W stosowanych przez przedsiębiorców telekomunikacyjnych wzorcach umownych zdarzają się bardzo wysokie z perspektywy konsumenta kary za nadużycia telekomunikacyjne (np. w wysokości 5000 zł), które uznawane były za klauzule abuzywne m.in. ze względu na zbyt ogólne sformułowanie przesłanek określających, czy doszło do nadużycia. Tego typu sytuację należałoby ocenić jako niekorzystną dla konsumentów.  W związku z powyższym wydaje się, że byłoby uzasadnione przyjęcie szczegółowych rozwiązań dopasowanych do zwalczania sztucznego ruchu, przewidujących jednocześnie możliwość ochrony konsumentów przed nieproporcjonalnym lub omyłkowym działaniem przedsiębiorców telekomunikacyjnych, np. przez udzielenie im odpowiednich informacji o podstawie podjęcia działań przez operatora oraz umożliwienie powtórnej weryfikacji sytuacji. | **Uwaga nieuwzględniona**  Do zjawiska sztucznego ruchu będzie miał zastosowanie ogólny przepis nakładający obowiązek stosowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Problemy wskazane w uwadze mogą zostać przezwyciężone w drodze postępowania reklamacyjnego, czy postępowań ADR prowadzonych przez Prezesa UKE. Nie jest uzasadnione wprowadzanie szczególnej regulacji, np. obowiązku informacyjnego, tylko i wyłącznie w związku z zapobieganiem i zwalczaniem zjawiska sztucznego ruchu. |
|  | DC UKNF | Art. 2 pkt 4 | Definicja nadużycia w komunikacji elektronicznej odnosi się do użytkownika końcowego, którym zgodnie z art. 2 pkt 50 ustawy Prawo telekomunikacyjne jest podmiot korzystający z publicznie dostępnej usługi telekomunikacyjnej lub żądający świadczenia takiej usługi, dla zaspokojenia własnych potrzeb. W praktyce można spotkać się zaś z przypadkami, w których atak cyberprzestępców dokonywany jest na osobę fizyczną, np. pracownika instytucji państwowej lub podmiotu gospodarczego, w celu wyrządzenia szkody tej instytucji bądź podmiotowi gospodarczemu. Dotyczy to zarówno sytuacji, gdy ofiara ataku korzysta z urządzenia służbowego oraz usługi telekomunikacyjnej, której abonentem jest pracodawca, jak i przypadku, w którym atak nakierowany jest na prywatne urządzenia użytkownika i wykorzystywane przez niego prywatne usługi telekomunikacyjne. Użycie w ramach omawianego przepisu terminu „użytkownik końcowy” może powodować konieczność doprecyzowania jego treści tak, aby objęte nim były również rodzaje przypadków zasygnalizowane powyżej. | **Uwaga wyjaśniona w zakresie pojęcia użytkownika końcowego**  W pierwszym opisanym przypadku nadużycie w komunikacji elektronicznej jest kierowane przeciwko instytucji państwowej, która jest użytkownikiem końcowym. W drugim przypadku nadużycie jest wobec pracownika tej instytucji, przy wykorzystaniu jego prywatnych urządzeń – pracownik też jest użytkownikiem końcowym. |
|  | UOKIK | Art. 2 pkt 4 | Art. 2 pkt 4  W projekcie pojawia się definicja nadużycia w komunikacji elektronicznej, rozumianego jako świadczenie 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. W art. 2 pkt 12 projektu zdefiniowano także usługę komunikacji interpersonalnej, a w art. 2 pkt 13 z kolei usługę komunikacji interpersonalnej niewykorzystującą numerów.  Niezbędne jest wskazanie, że zgodnie z art. 2 pkt 48 ustawy z 16 lipca 2004 r. Prawo telekomunikacyjne (Dz. U. z 2022 r. poz. 501), usługę telekomunikacyjną określa się jako usługę polegającą głównie na przekazywaniu sygnałów w sieci telekomunikacyjnej. Tym samym definicja nadużycia w komunikacji elektronicznej odnosi się wyłącznie do wąskiej definicji usługi telekomunikacyjnej i pomija definicje usługi komunikacji interpersonalnej i komunikacji interpersonalnej niewykorzystującej numerów. Wydaje się, że tego typu wąskie zakreślenie zakresu przedmiotowego art. 2 pkt 4 projektu nie jest wskazane i być może rozważyć należałoby jego rozszerzenie o dodatkowe definicje. | **Uwaga nieuwzględniona**  Szersza definicja w ustawie jest niezbędna z powodu wprowadzenia przepisów dotyczących poczty elektronicznej. Z uwagi na wykorzystywanie w komunikacji elektronicznej również szyfrowania end-to-end, które sprawia, że wykrywanie części nadużyć byłoby niemożliwe, a także kwestie prywatności w komunikacji, nie proponuje się objęcia tej komunikacji szczególnymi rozwiązaniami w projekcie ustawy. |
|  | DC UKNF | Art. 3 ust. 1 pkt 2 | Zakaz sformułowany w art. 3 ust. 1 pkt 2 projektu ustawy obejmuje wiadomości SMS, jednak poza jego zakresem pozostają wiadomości EMS i MMS. Jeżeli technicznie możliwe jest wykorzystanie wiadomości EMS lub MMS w celach wskazanych w w/w przepisie, a także blokowanie tego rodzaju wiadomości przez przedsiębiorców telekomunikacyjnych, to zasadnym wydaje się rozszerzenie zakresu omawianego zakazu również na wiadomości EMS i MMS. Postulat ten uzasadniony jest również doświadczeniami UKNF w zakresie monitorowania negatywnych zjawisk na rynku finansowym oraz im przeciwdziałania. Znane są bowiem przypadki wykorzystywania wiadomości MMS w celu podszycia się przez nadawcę pod inny podmiot, aby nakłonić odbiorcę takiej wiadomości do określonego działania (w szczególności przekazania danych osobowych czy rozporządzenia majątkiem).  W przypadku uwzględnienia niniejszej uwagi, uzasadnione będą także zmiany dostosowujące w: art. 1 pkt 2, art. 4 ust. 1-3 oraz 5-6, art. 5 ust. 1 i 2, art. 6 ust. 1 pkt 2, art. 7, art. 14 ust. 2 oraz ust. 3 pkt 1, oraz art. 16 ust. 1 pkt 2. | **Uwaga częściowo uwzględniona**  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. |
|  | DC UKNF | Art. 3 ust. 1 pkt 2 oraz art. 16 ust. 1 pkt 2 | Omawiany zakaz odnosi się do wysyłania SMS, w których nadawca podszywa się pod inny podmiot w celu nakłonienia odbiorcy od określonego działania, m.in. nieświadomego rozporządzenia majątkiem. Omawiany katalog działań, do których nakłaniać może nadawca, ma co prawda charakter otwarty, jednak sugerujemy rozważenie zastąpienia terminu „nieświadomego” (w ramach w/w sformułowania) terminem „niekorzystnego” rozporządzenia majątkiem. Nieświadomy oznacza bowiem niezdający sobie z czegoś sprawy, powstały bez udziału świadomości. Zmiana ta pozwoli uniknąć wątpliwości, że zakaz rozciąga się również na nakłanianie, poprzez podszywanie się pod inny podmiot, do rozporządzenia majątkiem, które jest świadome ale niekorzystne dla ofiary ataku. Sama czynność rozporządzenia majątkiem będzie zazwyczaj dokonywana pod wpływem błędu, który wywołał sprawca. Również znamiona przestępstwa oszustwa (art. 286 k.k.) nie wymagają braku „świadomości” działania pokrzywdzonego, a odnoszą się one do niekorzystnego rozporządzenia mieniem.  Omawiana uwaga odnosi się również do art. 16 ust. 1 pkt 2 projektu ustawy. | **Uwaga nieuwzględniona**  Zawarte w ustawie brzmienie lepiej oddaje istotę nadużyć w telekomunikacji elektronicznej. Istotą smishingu jest podszycie pod inny podmiot i doprowadzenie użytkownika do dokonania czynności, której konsekwencji nie jest świadom. W ramach normalnego obrotu gospodarczego dochodzi z kolei do wielu transakcji gdzie można mówić o niekorzystnym rozporządzeniu majątkiem, ale jeśli osoba dokonująca danej czynności jest świadoma jej konsekwencji to nie mamy do czynienia z przestępstwem. Z powyższych względów pozostawiono dotychczasowe brzmienie przepisu. |
|  | DC UKNF | Art. 3 ust. 1 pkt 3 | W zakresie użytego w tym przepisie terminu „nieświadomego rozporządzenia majątkiem” postulujemy rozważenie zastąpienia go terminem „niekorzystnego rozporządzenia majątkiem”, z tożsamych przyczyn jak wskazane w w/w uwadze do art. 3 ust. 1 pkt 2 projektu ustawy. | **Uwaga nieuwzględniona**  Zawarte w ustawie brzmienie lepiej oddaje istotę nadużyć w telekomunikacji elektronicznej. Istotą smishingu jest podszycie pod inny podmiot i doprowadzenie użytkownika do dokonania czynności, której konsekwencji nie jest świadom. W ramach normalnego obrotu gospodarczego dochodzi z kolei do wielu transakcji gdzie można mówić o niekorzystnym rozporządzeniu majątkiem, ale jeśli osoba dokonująca danej czynności jest świadoma jej konsekwencji to nie mamy do czynienia z przestępstwem. Z powyższych względów pozostawiono dotychczasowe brzmienie przepisu. |
|  | UOKIK | Art. 4 ust. 2 | **4 ust. 2**  Prezes UOKiK popiera ogólny kierunek wprowadzonych rozwiązań legislacyjnych, a także wspiera zmiany regulacyjne, które pozwolą na skuteczną walkę ze zjawiskiem smishingu.  Jednocześnie należy wskazać, że według założeń omawianego przepisu, CSIRT NASK będzie posiadać bardzo dużą uznaniowość odnośnie do tworzenia wzorca wiadomości  wyczerpującej znamiona smishingu. Wzorzec ten posłużyć ma w następnej kolejności do rozpoczęcia przez przedsiębiorców telekomunikacyjnych niezwłocznego blokowania krótkich wiadomości tekstowych (SMS) zawierających treści zawarte we wzorcu wiadomości.  Prezes UOKiK stale otrzymuje różnorodne sygnały ze strony konsumentów oraz przedsiębiorców, dotyczące bardzo szerokiego spektrum praktyk rynkowych i zagadnień, wliczając w to liczne zgłoszenia dotyczące sfery telekomunikacji i e-commerce. Prezes UOKiK jest podmiotem, który regularnie styka się zatem z przejawami nadużyć w komunikacji elektronicznej, zarówno noszącymi znamiona smishingu i spoofingu, jak i innymi. W związku z powyższym istnieje możliwość, że Prezes UOKiK wejdzie w posiadanie informacji na temat praktyki lub zjawiska w telekomunikacji niezgodnego z prawem, zgłoszenie którego do CSIRT NASK może być uzasadnione, w tym na przykład identyfikacji wiadomości noszącej znamiona smishingu. Wydaje się zatem zasadne, aby CSIRT NASK zobowiązany był do udzielenia pisemnej odpowiedzi Prezesowi UOKiK w przypadku uznania, że dana wiadomość nie stanowi smishingu. Uzasadnienie odmownej decyzji pozwoliłoby to Prezesowi UOKiK na zdobycie informacji z zakresu nadużyć telekomunikacyjnych, a tym samym lepsze wykonywanie jego funkcji i potencjalne zwiększenie poziomu ochrony konsumentów w Polsce. | **Uwaga nieuwzględniona**  Nie jest w ocenie projektodawcy zasadne tak dokładne ukształtowanie zasad współpracy pomiędzy różnymi podmiotami administracji publicznej. Każdy podmiot posiadający informacje o występujących przypadkach smishingu może poinformować o tym CSIRT NASK. Takie działania mieszczą się w ramach normalnego funkcjonowania podmiotów publicznych i nie wymagają uściślenia w ustawie.  Należy również zauważyć, że każdy będzie mógł zapoznać się ze wzorcem wiadomości wyczerpującej znamiona smishingu po jego udostępnieniu na stronie internetowej, a nadawca zablokowanej wiadomości SMS, będzie mógł wnieść sprzeciw do Prezesa UKE.  W związku z powyższym proces tworzenia i publikacji wzorców smishingowych został kompleksowo uregulowany i nie wymaga zmian, o których mowa w uwadze. |
|  | DC UKNF | Art. 4 ust. 4 | Przepis przewiduje udostępnianie na stronie internetowej CSIRT NASK wzorców wiadomości wyczerpujących znamiona smishingu. Udostępnianie tego rodzaju wzorców wiąże się w ocenie UKNF z ryzykiem wykorzystania tych informacji przez przestępców do przygotowywania wiadomości, które będą odróżniały się od opublikowanych wzorców, w celu ominięcia zabezpieczeń. Sugerujemy rozważenie usunięcia omawianego przepisu i pozostawienie sposobu przekazywania informacji o wzorcach tego typu wiadomości w sposób przewidziany w projektowanym art. 4 ust. 3, podmiotom w nim wskazanym, pozostawiając wzorce poza możliwością publicznego do nich dostępu. | **Uwaga nieuwzględniona**  Jawność wzorca wiadomości smishingowej jest niezbędna dla zapewnienia przejrzystości procesu blokowania wiadomości a także jest niezbędna dla zagwarantowania praw użytkowników i możliwości skorzystania z instytucji sprzeciwu przez nadawcę wiadomości, która została zablokowana jako wpisująca się we wzorzec. |
|  | UOKIK | Art. 4 ust. 4 | Art. 4 ust. 4  Przepis wskazuje, że wzorzec wiadomości wyczerpującej znamiona smishingu, CSIRT NASK udostępnia na swojej stronie internetowej, w terminie 14 dni nie później jednak niż w terminie 21 dni od dnia jego przekazania przedsiębiorcy telekomunikacyjnemu.  Z perspektywy Prezesa UOKiK, powyższe terminy są relatywnie długie, jeśli chodzi o kwestie cyberbezpieczeństwa i ochrony konsumentów. Należy także zauważyć, że mimo obowiązku niezwłocznego blokowania tego typu wiadomości przez przedsiębiorcę (art. 4 ust. 6), istnieje ryzyko modyfikacji treści wiadomości przez jej autora i dalszego jej wysyłania, przy zachowaniu zbliżonej treści lub sposobu jej sformułowania. Tym samym jak najwcześniejsza możliwość zapoznania się ze wzorcem takiej wiadomości może być korzystna z punktu widzenia ochrony jej potencjalnych odbiorców. Dzięki temu możliwe byłoby także przekazanie informacji na temat danego przypadku i stosowanej metody smishingu do publicznej wiadomości. Warto zatem rozważyć skrócenie wskazanych w projekcie terminów udostępnienia wzorca wiadomości przez CSIRT NASK na jego stronie internetowej. Można także zauważyć, że uzasadnienie projektu nie odnosi się w jakikolwiek sposób do wskazanych terminów i trudno ocenić, na jakiej podstawie zostały określone, a także czy ich długość jest uzasadniona ograniczeniami technologicznymi. | **Uwaga wyjaśniona**  Opisany mechanizm dotyczy publikacji wzorca dla wszystkich odbiorców, a nie jego przekazania do przedsiębiorców telekomunikacyjnych. Przekazanie wzorca do przedsiębiorcy następuje niezwłocznie po jego zidentyfikowaniu 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 zmienić stosowane przez nich wiadomości i mogłoby to sprawić, że ustawa nie zrealizuje swojego celu. |
|  | UKE | Art. 4 ust. 5 | Art. 4 ust. 5 – proponuje się doprecyzować pojęcie „niecelowości” (blokowania SMS). Jest to o tyle istotne, że w art. 4 ust. 6 pkt 2 ponownie użyte jest to pojęcie w kontekście obowiązku ciążącego na przedsiębiorcy telekomunikacyjnym, za którego niewykonanie przewidziano karę pieniężną w art. 15 ust. 2 pkt 1 projektu. W omawianym przepisie należy również skreślić wyraz „uzna”, który jest zbędny, a nadto sugeruje arbitralność decyzji CSIRT NASK. | **Uwaga częściowo uwzględniona**  **w zakresie pojęcia niecelowości.** Pojęcie niecelowości zostanie wyjaśnione w uzasadnieniu.  Niecelowe jest dalsze blokowanie krótkich wiadomości tekstowych (SMS), jeżeli pomimo wzorca:  smishing dociera do użytkowników i wzorzec musi być poprawiony lub  wzorzec jest zbyt szeroki i blokuje także sms nie mające charakteru smishingu, a także gdy  oszuści już nie korzystają z wcześniejszych metod w smishingu, np. nie używają sformułowań związanych ze szczepieniem. Wzorzec może być wycofany. **Uwaga nieuwzględniona w pozostałym zakresie**  Nie ma konieczności usunięcia wyrazu „uzna” – CSIRT NASK dokonuje subsumpcji i kwalifikuje sms jako zawierający treści o charakterze smishingu w oparciu o przepisy prawa. |
|  | UOKIK | Art. 7 | Art. 7  Zgodnie z treścią tego przepisu, przedsiębiorca telekomunikacyjny może blokować krótkie wiadomości tekstowe (SMS) zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości CSIRT NASK.  W ocenie Prezesa UOKiK istnieją określone zagrożenia związane z uznaniowym charakterem uprawnienia, w jakie wyposażeni zostają przedsiębiorcy w omawianym zakresie. Nie istnieją żadne reguły dotyczące blokowania wiadomości SMS przez przedsiębiorców na podstawie tego przepisu. Istnieje zatem ryzyko stosowania przez nich arbitralnych kryteriów oceny danej wiadomości, stanowiących podstawę podjęcia decyzji o blokowaniu krótkiej wiadomości tekstowej.  Prezes UOKiK w swojej działalności obserwuje różnego rodzaju nieprawidłowości, których dopuszczają się nie tylko podmioty trzecie względem dostawców usług telekomunikacyjnych (niepowiązane z nimi), lecz także kontrahenci przedsiębiorców telekomunikacyjnych świadczący np. usługi rozliczane w modelu direct billing (doliczania do rachunku) lub usługi premium, w ramach których część korzyści ze świadczenia usługi czerpie również przedsiębiorca telekomunikacyjny. W przeszłości zdarzały się przypadki braku stosownej reakcji na sygnalizowane przez konsumentów nieprawidłowości związane z różnego rodzaju kampaniami SMS-owymi prowadzonymi przez kontrahentów przedsiębiorców telekomunikacyjnych1. Ustalenie zasad blokowania wiadomości jednolitych dla różnego rodzaju nadużyć mogłoby być zasadne, z uwagi na potrzebę zapewnienia równych standardów traktowania dla wszystkich uczestników rynku.  Wskazane byłoby także udzielenie informacji konsumentowi na temat zablokowania danej wiadomości i wskazanie, z jakich przyczyn została zablokowana. Adresat miałby dzięki temu świadomość, że została do niego skierowana wiadomość, która jednak w ocenie przedsiębiorcy nosiła znamiona smishingu. Jednocześnie mógłby dzięki temu zakwestionować decyzję operatora, jeśli jego zdaniem została zaklasyfikowania jako smishing błędnie i powinna zostać dostarczona, co ograniczyłoby negatywne skutki ewentualnych błędów przy realizacji ww. obowiązków. Uwzględniając, że art. 7 daje przedsiębiorcy możliwość uznaniowego, arbitralnego klasyfikowania wiadomości SMS, tego typu sytuacje mogą mieć miejsce. Dlatego wydaje się, że wprowadzenie obowiązku informowania konsumenta przez przedsiębiorcę byłoby uzasadnione. | **Uwaga nieuwzględniona**  Przedsiębiorcy telekomunikacyjni będą podlegali odpowiedzialności kontraktowej za niewykonanie usługi. Kwestie te powinny zostać rozstrzygnięte w ramach postępowania reklamacyjnego, prowadzonego przez Prezesa UKE postępowania ADR, czy w związku z postanowieniami umownymi. |
|  | UKE | Art. 8 | Art. 8 – rekomenduje się użycie w tym przepisie zwrotu „eliminacja prezentacji identyfikacji numeru wywołującego”, by w największym możliwym stopniu zapewnić zgodność terminologiczną projektowanego przepisu z art. 171 Prawa telekomunikacyjnego. Poza tym omawiany przepis nie określa dostatecznie jasno zakresu stosowania ustanowionej w nim normy. Z dosłownego jego brzmienia odnieść można wrażenie, że przedsiębiorca telekomunikacyjny zawsze ma blokować połączenie głosowe albo ukrywać identyfikację numeru wywołującego dla użytkownika końcowego. Dlatego poddaje się pod rozwagę, aby treść przepisu rozpoczynała się np. od wyrazów: „W przypadku uzasadnionego podejrzenia CLI spoofingu (...)” | **Uwaga częściowo uwzględniona**  Zamiast „informacji adresowej” zostanie użyte sformułowanie „ukrycie informacji numeru wywołującego”.  Należy zauważyć, że art. 8 ustanawia ogólny obowiązek blokowania połączeń głosowych w ramach zwalczania i przeciwdziałanie spoofingowi. Użyte sformułowanie jest najbardziej ogólne tak aby objąć całość działalności przedsiębiorców telekomunikacyjnych w tym zakresie. Przepis ten musi również być odczytywany w kontekście całej ustawy, a zwłaszcza przepisów mówiących o porozumieniu między przedsiębiorcami telekomunikacyjnymi a Prezesem UKE. W związku z tym opisywane w tym przepisie działanie będzie wynikało z wprowadzonych środków technicznych i organizacyjnych służących przeciwdziałaniu nadużyciom w telekomunikacji elektronicznej. W związku z powyższym nie jest konieczne doprecyzowanie tego przepisu. |
|  | UOKIK | Art. 8 | Art. 8  W opinii Prezesa UOKiK, wskazany przepis budzi wątpliwości interpretacyjne w odniesieniu do sformułowania „ukrywa identyfikację numeru wywołującego dla użytkownika końcowego”. Wskazane byłoby wyjaśnienie, jak należy rozumieć to stwierdzenie. Czy chodzi tu o ukrycie numeru przez operatora w taki sposób, że numer telefonu udający numer innego podmiotu miałby nie być pokazywany na wyświetlaczu odbiorcy? Opisane sformułowanie może być interpretowane na różne sposoby, a w takiej sytuacji jego doprecyzowanie może pozwolić na zwiększenie przejrzystości omawianego przepisu.  W ramach propozycji, można zasugerować zmianę sformułowania na „ukrywa nieprawdziwą identyfikację numeru wywołującego dla użytkownika końcowego”. | **Uwaga wyjaśniona**  Tak, chodzi o ukrycie numeru przez operatora w taki sposób, że numer telefonu udający numer innego podmiotu miałby nie być pokazywany na wyświetlaczu odbiorcy (per analogiam jak działa usługa CLIR). Ukrycie prezentacji identyfikacji linii wywołującej oznacza w praktyce, że odbiorcy wyświetli się, że dzwoni do niego nieznany numer a nie np. informacja, ze dzwoni osoba bliska, której numer jest wpisany na liście kontaktów. Pozwoli to zapobiec takim atakom jak np. podszycie się pod byłego szefa CBA Pawła Wojtunika. |
|  | UKE | Art. 9 ust. 1 | Art. 9 ust. 1 - proponuje się wykorzystanie do prowadzenia wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych systemu teleinformatycznego, o którym mowa w art. 29b ust. 2 ustawy z dnia 7 maja 2010 r. o wspieraniu rozwoju usług i sieci telekomunikacyjnych, po dokonaniu jego rozbudowy o wymaganą do tego funkcjonalność. Proponowane rozwiązanie zapewni udostępnienie pełnego wykazu do pobrania (w odpowiednim formacie) wyłącznie zweryfikowanym i podłączonym do tego systemu przedsiębiorcom telekomunikacyjnym, na potrzeby implementacji rozwiązań służących zapobieganiu i zwalczaniu CLI spoofingu. Z kolei podmiotom innym niż przedsiębiorcy telekomunikacyjni, w szczególności abonentom wnioskującym o wpis wykorzystywanego przez siebie numeru do wykazu, o którym mowa w art. 9 ust. 1 projektu, powinna być jedynie zapewniona możliwość wglądu do tego wykazu i to tylko w zakresie obejmującym wpisane numery (tzn. bez danych podmiotów, które te numery wykorzystują). Powyższe mogłoby nastąpić np. poprzez udostępnienie zanonimizowanych danych z wykazu, o którym mowa w art. 9 ust. 1 projektu, w Biuletynie Informacji Publicznej na stronie podmiotowej Prezesa UKE.  Niezależnie od powyższego z ust. 1 należy wykreślić wyraz „telefonów”, by zapewnić spójność terminologiczną z Prawem telekomunikacyjnym. | **Uwaga uwzględniona w zakresie wykreślenia wyrazu „telefonów”**  **W pozostałym zakresie uwaga nieuwzględniona**  W ocenie projektodawcy, nie jest zasadne wskazywanie konkretnego systemu teleinformatycznego w tym przepisie, a zapewnić możliwość jak najłatwiejszej i jak najmniej obciążającej zarówno Urząd jak i przedsiębiorców telekomunikacyjnych integracji w celu wykonania postanowień ustawy. |
|  | DC UKNF | Art. 9 ust. 2 | Katalog podmiotów uprawnionych do złożenia wniosku o wpis do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych obejmuje obecnie jednostki sektora finansów publicznych oraz banki. Zagrożenie związane ze spoofingiem dotyczy zaś szerszej kategorii podmiotów rynku finansowego. Podwyższone ryzyko „podszywania się” z wykorzystaniem spoofingu dotyczy przede wszystkim tych podmiotów, które prowadzą rachunki (bankowe, płatnicze lub papierów wartościowych), świadczą usługi płatnicze, bądź prowadzą działalność inwestycyjną (lokują środki pieniężne zebrane w drodze proponowania nabycia jednostek uczestnictwa albo certyfikatów inwestycyjnych w określone w ustawie papiery wartościowe, instrumenty rynku pieniężnego i inne prawa majątkowe) ale może również obejmować podmioty z sektora ubezpieczeniowego.  W związku z powyższym sugerujemy rozważenie poszerzenia omawianego katalogu o możliwość złożenia wniosku przez inne podmioty sektora finansowego szczególnie narażone na spoofing. Dotyczy to przede wszystkim następujących podmiotów, podlegających nadzorowi KNF lub nadzorowi państwa macierzystego (jak w przypadku oddziałów instytucji kredytowych):   1. spółdzielczej kasy oszczędnościowo-kredytowej lub Krajowej Kasy Oszczędnościowo-Kredytowej, 2. instytucji płatniczej, 3. firmy inwestycyjnej, 4. funduszu inwestycyjnego lub towarzystwa funduszy inwestycyjnych, 5. zakładu ubezpieczeń lub zakładu reasekuracji, 6. oddziału instytucji kredytowej.   Jednocześnie, ze względu na istotną rolę na rynku finansowym niektórych podmiotów pozostających poza nadzorem KNF, a także podwyższone ryzyko „podszycia się” pod takie podmioty w ramach ataku z użyciem spoofingu, sugerujemy rozważenie dodania do omawianego katalogu również tego rodzaju podmiotów (zastrzegając jednocześnie, że np. w przypadku podmiotów prowadzących systemy płatności istotna może być opinia Prezesa Narodowego Banku Polskiego sprawującego nadzór systemowy nad systemem płatniczym). Dotyczy to w szczególności następujących kategorii podmiotów:   1. bankowej izby gospodarczej, 2. podmiotu prowadzącego system płatności, 3. instytucji utworzonej na mocy art. 105 ust. 4 ustawy z dnia z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j. Dz. U. z 2021 r. poz. 2439 z późn. zm.).   Poddajemy pod rozwagę delegowanie katalogu podmiotów uprawnionych do złożenia w/w wniosku do Rozporządzenia Prezesa RM, co w opinii Urzędu KNF usprawni proces zarządzania katalogiem uprawnionych podmiotów w przypadku konieczności jego aktualizacji. | **Uwaga częściowo uwzględniona** Dodane zostaną kategorie podmiotów, które są nadzorowane przez KNF.  **Uwaga nieuwzględniona w zakresie podmiotów uprawnionych do złożenia ww. wniosku do rozporządzenia Prezesa RM** Takie rozwiązanie nie wydaje się adekwatne, biorąc pod uwagę, że adresaci uprawnień i obowiązków, to co do zasady, powinny zostać określeni w przepisach rangi ustawowej. |
|  | DC UKNF | Art. 9 ust. 4 | Wniosek o wpis numeru do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych ma zawierać jedynie oznaczenie podmiotu, od którego pochodzi oraz numeru, który ma służyć wyłącznie do odbierania połączeń głosowych. Brak jest natomiast przewidzianego środka weryfikacji, czy zgłaszany numer w rzeczywistości należy do wnioskodawcy. Można rozważyć w tym zakresie wymóg załączenia aktualnej umowy na usługi telekomunikacyjne dotyczące omawianego numeru bądź weryfikację przez Prezesa UKE u przedsiębiorcy telekomunikacyjnego prowadzącego numer (wtedy należałoby przewidzieć wymóg wskazywania takiej informacji we wniosku). Brak wprowadzenia środka weryfikacji uprawnienia wnioskodawcy do zgłaszanego przez niego numeru telefonu może bowiem kreować ryzyko złośliwego/nieuprawnionego zablokowania możliwości wykonywania połączeń z numerów telefonów podmiotów, o których mowa w projektowanym art. 9 ust. 2 ustawy.  Jednocześnie zwracamy uwagę, że Projekt nie obejmuje sytuacji, w której podmiot uprawniony przestaje korzystać ze zgłoszonej przez niego puli numeracyjnej (i nie informuje o tym fakcje Prezesa UKE). Pomimo zmiany abonenta pula numerów nadal jest blokowana. Może to doprowadzić do sytuacji pozyskania i dalszego wykorzystania przez podmiot nieuprawniony puli numeracyjnej z której korzystał uprzednio podmiot uprawniony, a która pozostaje wpisana w wykazie. | **Uwaga wyjaśniona**  Wykaz będzie jawny, więc będzie możliwość wycofania wniosku przez kolejny podmiot korzystający z numeracji. |
|  | UKE | Art. 9 ust. 8 | Art. 9 ust. 8 - sugeruje się rezygnację z formy decyzji administracyjnej dla odmowy dokonania wpisu do wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych. Wniosek niezgodny z art. 9 ust. 2 i 3 projektu powinien być pozostawiony przez organ bez rozpoznania, co uprości i odformalizuje procedurę odmowy dokonania wpisu do wykazu. Poza tym należy zauważyć, że przepis ust. 8 jest wadliwie skonstruowany, ponieważ wynika z niego, że przesłanką odmowy wpisu jest to, że numer jest niewykorzystywany przez podmiot nieuprawniony. | **Uwaga częściowo uwzględniona**  Usunięty zostanie wymóg decyzji administracyjnej dla odmowy dokonania wpisu do wykazu numerów. Ust. 8 zostanie poprawiony.  **Uwaga nieuwzględniona w pozostałym zakresie**  W zakresie numeru niewykorzystywanego należy zauważyć, że ust. 8 musi być czytany w kontekście całego art. 9. Na etapie składania wniosku, wnioskodawca musi przedstawić dowód, że numer wskazany we wniosku należy do niego. Na tym etapie jest to badane jedynie pod kątem formalnym. Sformułowanie o „niewykorzystywanym numerze” w ust. 8 jest za to podstawą do organu do zbadania pod kątem materialnym, czy rzeczywiście numer ten jest użytkowany przez dany podmiot. Z tego względu przepis w tym brzmieniu jest potrzebny. |
|  | UOKIK | Art. 10 ust. 1 | Art. 10 ust. 1  Art. 10 wskazuje jako jego adresatów operatorów, którzy mogą zawrzeć z Prezesem UKE porozumienie z zakresu realizacji obowiązków, o których mowa w art. 8. Art. 8 posługuje się wyłącznie terminem „przedsiębiorca telekomunikacyjny”, na którego nakłada obowiązek blokowania połączenia głosowego albo ukrywania identyfikacji numeru wywołującego dla użytkownika końcowego. Termin operator i przedsiębiorca telekomunikacyjny zostały zdefiniowane w art. 2 odmiennie i jako odrębne od siebie - art. 2 pkt 5) (operator) oraz art. 2 pkt 7 (przedsiębiorca telekomunikacyjny). Powstaje zatem nieścisłość terminologiczna między powiązanymi ze sobą przepisami. Powstaje zatem pytanie, czy jest to zabieg celowy i jak powinien być rozumiany. Niezbędne jest odniesienie się do tej kwestii. | **Uwaga częściowo uwzględniona**  **Przepis zostanie przeredagowany zgodnie z propozycją Prezesa UKE**  Porozumienie będzie mogło być zawarte zoperatorami zapewniającymi świadczenie usług dla co najmniej 50 000 abonentów. Dla pozostałych przedsiębiorców telekomunikacyjnych Prezes UKE powinien natomiast wydawać rekomendacje dotyczące środków organizacyjnych i technicznych, służących realizacji obowiązku, o którym mowa w art. 8 projektu. |
|  | DC UKNF | Art. 11 ust. 1, 4 i 6 | Zgodnie z art. 11 ust. 6 projektu ustawy, przedsiębiorca telekomunikacyjny może uniemożliwić użytkownikom Internetu dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1. Przepis ten sformułowany jest w formie uprawnienia, a nie obowiązku blokowania stron wpisanych na listę ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników Internetu. Uwzględniając skalę wykorzystywania omawianych stron do wyłudzeń oraz negatywne skutki, jakie wiąże się z ich funkcjonowaniem dla obywateli RP i podmiotów gospodarczych (w tym ich straty finansowe mogące sięgać dziesiątków milionów złotych) w ocenie UKNF zasadne jest nałożenie na przedsiębiorców telekomunikacyjnych obowiązku blokowania dostępu do omawianych stron. W związku z powyższym sugerujemy rozważenie zmiany treści art. 11 ust. 6 projektu ustawy i zastąpienie sformułowania „może uniemożliwić” terminem „uniemożliwia”.  Dodatkowo, projektowany art. 11 ust. 1 odnosi się do możliwości zawarcia porozumienia w zakresie prowadzenia i utrzymywania jawnej listy ostrzeżeń dotyczących domen internetowych, o których mowa powyżej. Ustęp 4 wymienionego przepisu wskazuje przy tym, że stronami takiego porozumienia są m.in. „przedsiębiorca telekomunikacyjny lub przedsiębiorcy telekomunikacyjni”. W kontekście omawianego sformułowania powstaje wątpliwość, czy zawarcie porozumienia pozostaje dla przedsiębiorców telekomunikacyjnych dobrowolne, czy też obowiązkowe. W ocenie UKNF zasadne jest doprecyzowanie omawianego przepisu, aby z jego treści wynikał obowiązek zawarcia omawianego porozumienia przez przedsiębiorców telekomunikacyjnych. Obligatoryjny charakter przystąpienia do omawianego porozumienia pozytywnie przyczyniłby się do skuteczności projektowanych w niniejszym przepisie rozwiązań. Przedmiotowe porozumienie reguluje bowiem m.in. zasady zgłaszania domen internetowych, a zasadnym jest udział w tym procesie również przedsiębiorców telekomunikacyjnych – dzięki porozumieniu i ustalonym w nim wiążącym zasadom współpracy mógłby on być zaś bardziej efektywny. | **Uwaga uwzględniona poprzez dodanie obligatoryjnego wymogu blokowania stron**  **Uwaga nieuwzględniona w zakresie nałożenia obowiązku przystąpienia do porozumienia**  W ocenie projektodawcy należy pozostawić przedsiębiorcom telekomunikacyjnym swobodę wyboru sposobu realizacji obowiązków związanych z przeciwdziałaniem nadużyć telekomunikacyjnych. Będą oni mogli wybrać inny sposób realizacji nałożonych na nich obowiązków, ale będzie się to wiązało z brakiem domniemania, że obowiązki są prawidłowo realizowane. |
|  | DC UKNF | Art. 11 ust. 1 | W celu zapewnienia, że ochronie podlegać będą również przypadki, w których rozporządzenia dokonuje np. pracownik przedsiębiorcy dysponujący jego majątkiem (przykładowo atak na księgowego spółki metodą „podszycia się” pod członka zarządu) sugerujemy usunięcie ze sformułowania „doprowadzającymi użytkowników Internetu do niekorzystnego rozporządzenia ich majątkiem” słowa „ich”. Jednocześnie, dla zachowania spójności ze zdaniem pierwszym (które odnosi się do majątku), sugerujemy rozważenie zastąpienia w zdaniu drugim omawianego przepisu terminu „środków finansowych” terminem „majątku” – jest to pojęcie szersze i mogą zdarzyć się ataki, w których wyłudzeniu podlegać będzie towar czy wykonanie usługi, a nie środki finansowe. Proponowane zmiany pozostają również zgodne z zaproponowaną w projekcie definicją CLI spoofing. | **Uwaga nieuwzględniona**  Mechanizm proponowany w ustawie funkcjonuje obecnie – jest nim lista ostrzeżeń przed niebezpiecznymi stronami prowadzona przez NASK-PIB[[1]](#footnote-2). |
|  | UKE | Art. 11 ust. 2 | Art. 11 ust. 2 – przepis wymaga przeredagowania, ponieważ przy obecnym brzmieniu niezrozumiały jest fragment „oraz uniemożliwienia dostępu do tych stron”. | **Uwaga wyjaśniona w związku z uwzględnieniem uwagi** Polskiego Towarzystwa Informatycznego Izba Rzeczoznawcówusunięty został przepis, którego uwaga dotyczy. |
|  | UKE | Art. 13 | Art. 13 – proponuje się rozważyć wprowadzenie do projektowanej ustawy kary pieniężnej za naruszenie tego przepisu, co powinno przyczynić się do zapewnienia przestrzegania obowiązków, o których w nim mowa. Ponadto w ust. 2 nie wskazano terminu początkowego przechowywania danych o usługach telekomunikacyjnych, które nie zostały przez przedsiębiorcę telekomunikacyjnego wykonane w związku z blokowaniem smishingu (powinno się go liczyć od dnia, w którym usługa miała być wykonana). | **Uwaga nieuwzględniona w zakresie kary**  Wprowadzenie kary pieniężnej za naruszenie przepisu art. 13 byłoby nieproporcjonalne względem obowiązków nałożonych na przedsiębiorcę.  Analogicznie do przepisów Prawa telekomunikacyjnego, zgodnie z którymi obowiązek rejestracji danych o wykonanych usługach telekomunikacyjnych, wyrażony w art. 168 PT nie podlega karze pieniężnej, przedsiębiorca musi zapewnić rozliczalność przed organami i abonentem. W przypadku projektowanej ustawy odnosi się to do sytuacji składania reklamacji względem niedostarczonej usługi.  Ponadto, należy wskazać, że przetwarzanie bez podstawy prawnej danych, o których mowa w art. 13, stanowiących dane osobowe, będzie podlegało sankcjom przewidzianym w RODO. |
|  | UKE | Art. 15 ust. 4 | Art. 15 ust. 4 – odesłanie do przepisów Prawa telekomunikacyjnego trzeba rozszerzyć o ust. 11 w art. 209. | **Uwaga wyjaśniona:**  Zmieniono brzmienie ust. 4 i obecnie nie zawiera on odesłania do przepisów PT.  Przepis otrzymał brzmienie:  4. Kara, o której mowa w ust. 1-3, może zostać nałożona także w przypadku, gdy podmiot zaprzestał naruszania prawa lub naprawił wyrządzoną szkodę, jeżeli Prezes UKE uzna, że przemawiają za tym czas trwania, zakres lub skutki naruszenia. |
|  | UKE | Art. 15 ust. 5 | Art. 15 ust. 5 – po pierwsze, wskazać należy, że kara pieniężna w wysokości do jednokrotności przeciętnego wynagrodzenia wydaje się karą niską, która może nie spełnić funkcji prewencyjnej i represyjnej kary. Po drugie, w ust. 5 występuje błędne odesłanie do art. 11 ust. 2. | **Uwaga częściowo uwzględniona**  Zmieniona została wysokość kary, jaka może zostać nałożona przez Prezesa UKE na kierującego przedsiębiorstwem – do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy.  Zmieniona została także sama konstrukcja przepisu, który  otrzymał brzmienie:  5. Niezależnie od kar pieniężnych, o których mowa w ust. 1 i 2, Prezes UKE może nałożyć na kierującego przedsiębiorstwem telekomunikacyjnym, w szczególności osobę pełniącą funkcję kierowniczą lub wchodzącą w skład organu zarządzającego przedsiębiorcy telekomunikacyjnego lub związku takich przedsiębiorców, karę pieniężną w wysokości do 300% jego miesięcznego wynagrodzenia, naliczanego jak dla celów ekwiwalentu za urlop wypoczynkowy. |

1. <https://cert.pl/posts/2020/03/ostrzezenia_phishing/> [↑](#footnote-ref-2)