|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| FLp. | | Instytucja | Jednostka redakcyjna | Treść uwagi | Odniesienie |
|  | | MSUE | Uwaga ogólna | 1. Projektowana ustawa nakłada określone obowiązki na przedsiębiorców telekomunikacyjnych i dostawców poczty elektronicznej (art. 3 ust. 2 6, art. 8, art., 12, art. 13 i art. 21 projektu). Mogą one w mojej opinii zostać uznane za zasady dotyczące usług w rozumieniu art. 1 ust. 1 lit. e) *dyrektywy (UE) 2015/1535 Parlamentu Europejskiego i Rady z dnia 9 września 2015 r. ustanawiającej procedurę udzielania informacji w dziedzinie przepisów technicznych oraz zasad dotyczących usług społeczeństwa informacyjnego*, których projekt podlega obowiązkowi notyfikacji zgodnie z procedurą określoną w tej dyrektywie.   Na mocy art. 1 ust. 3 dyrektywy 2015/1535 nie ma ona wprawdzie zastosowania do zasad odnoszących się do zagadnień objętych przepisami Unii w dziedzinie usług telekomunikacyjnych, jak jednak wskazano w uzasadnieniu projektu, materia regulowana projektowaną ustawą nie jest objęta przepisami *dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej*. Przywołane wyłączenie nie będzie miało zatem zastosowania w omawianym przypadku.  Decyzję o konieczności notyfikacji podejmuje projektodawca, w przypadku wątpliwości możliwe jest zasięgnięcie w tej kwestii opinii ministra właściwego do spraw gospodarki, który pełni funkcję koordynatora krajowego systemu notyfikacji norm i aktów prawnych.  Na marginesie powyższej uwagi pragnę dodatkowo zauważyć, że porozumienie pomiędzy Prezesem Urzędu Komunikacji Elektronicznej, a operatorami, o którym mowa w art. 10 ust. 1 projektu, może z kolei zostać uznane za przepis techniczny de facto zdefiniowany w art. 1 ust. 1 lit. f) ppkt (ii) dyrektywy 2015/1535. Jego projekt powinien zatem również zostać notyfikowany Komisji Europejskiej. | **Uwaga uwzględniona**  W związku z uwagami zgłoszonymi w ramach uzgodnień, aby holistycznie adresować zagadnienia związane z nadużyciami, do projektu ustawy zostaną przeniesione niektóre regulacje projektu ustawy - Prawo komunikacji elektronicznej, a więc również wdrożenie art. 97 ust. 2 dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej. W związku z powyższym regulacje zawarte w projekcie ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (włącznie z instytucją porozumieniem jako realizacją postanowień ustawy) skorzysta z wyłączenia na mocy art. 1 ust. 3 dyrektywy 2015/1535. |
|  | | MKSS | Uwaga Ogólna | W tym miejscu należy zwrócić uwagę, że w ramach realizacji ustawowych zadań służby specjalne wykonują czynności operacyjno-rozpoznawcze, które mogą polegać na podejmowaniu działań określonych w art. 3 ust. 1 projektowanej ustawy, penalizowanych w projektowanych art. 15 ust. 1 oraz art. 16 ust. 1 tej ustawy. Jednocześnie, mając na uwadze fakt, że czynności te są realizowane w celu wykonywania zadań ustawowych związanych z rozpoznawaniem zagrożeń dla bezpieczeństwa państwa albo wykrywaniem przestępstw i ścigania ich sprawców, celem uniknięcia ewentualnych wątpliwości interpretacyjnych, zasadne jest ustawowe wyłączenie osoby udzielającej pomocy funkcjonariuszowi oraz samego funkcjonariusza tych służb spod zakresu ww. odpowiedzialności karnej. | **Uwaga wyjaśniona**  Nie jest konieczne uregulowanie tych kwestii w przedmiotowej ustawie. Należy podkreślić, że wszystkie czyny penalizowane w niniejszej ustawie mają wyraźnie określony cel, co sprawia, że funkcjonariusze służb dokonując ich w ramach swoich obowiązków nie będą karani. Ponadto wszelkie tego typu działania powinny podlegać kontroli sądowej a funkcjonariusze powinni być do nich stosownie upoważnieni. |
|  | | RCL | Uwaga ogólna | w związku z otrzymanym do uzgodnień międzyresortowych projektem *ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (RD402)* Rządowe Centrum Legislacji na wstępie uprzejmie informuje, że w przypadku przedmiotowego projektu ustawy wyjaśnienia wymaga miejsce jakie Projektodawca przewiduje dla projektowanej regulacji w systemie prawa, a także wzajemne relacje projektowanej regulacji z ustawami regulującymi takie dziedziny spraw, jakimi są telekomunikacja i usługi świadczone drogą elektroniczną.  Powyższa kwestia wymaga wyjaśnienia, gdyż przedmiotowy projekt swoim zakresem wkracza w materię regulowaną ustawą z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576, z późn. zm.), dalej jako „*ustawa – Prawo telekomunikacyjne*”, której zakres przedmiotowy obejmuje m.in. prawa i obowiązki przedsiębiorców telekomunikacyjnych (art. 1 ust. 1 pkt 2 tej ustawy), warunki przetwarzania danych w telekomunikacji i ochrony tajemnicy telekomunikacyjnej (art. 1 ust. 1 pkt 9 tej ustawy), a także warunki ochrony użytkowników usług, w szczególności w zakresie prawa do prywatności i poufności (art. 1 ust. 1 pkt 7 tej ustawy). Projektowana regulacja dotyczy, jak się również wydaje, także kwestii związanych ze świadczeniem usług drogą elektroniczną, regulowanych przepisami ustawy z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną (Dz. U. z 2020 r. poz. 344).  Kwestia wykazania zasadności potrzeby odrębnej regulacji jest istotna, gdyż zgodnie z § 2 Zasad techniki prawodawczej ustawa powinna wyczerpująco regulować daną dziedzinę spraw, nie pozostawiając poza zakresem swego unormowania istotnych fragmentów tej dziedziny. Mając więc na uwadze zakres przedmiotowy i podmiotowy ustawy – Prawo telekomunikacyjne, zasadnym wydaje się wprowadzenie projektowanych regulacji dotyczących zwalczania nadużyć w komunikacji elektronicznej do ustawy regulującej ogół zagadnień dotyczących telekomunikacji i rezygnację z regulacji odrębnej.  Obecnie ustawą podstawową dla tej dziedziny spraw jest ustawa – Prawo telekomunikacyjne, ale w tym miejscu przypomnieć należy, że trwają zaawansowane prace legislacyjne nad regulacją ustawową dotyczącą komunikacji elektronicznej, w tym działalności telekomunikacyjnej, która zawiera przepisy dotyczące nadużyć telekomunikacyjnych (art. 173 projektu ustawy - Prawo komunikacji elektronicznej, UC45).  Ponadto wskazać należy, że procedowana równolegle *ustawa – Przepisy wprowadzające ustawę - Prawo komunikacji* elektronicznej uchyla ustawę - Prawo telekomunikacyjne, do której przepisów odsyła, i na której bazuje, opiniowany projekt ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Wejście w życie *ustawy Przepisy wprowadzające ustawę - Prawo komunikacji elektronicznej* oraz *ustawy - Prawo komunikacji elektronicznej* spowodują więc konieczność zasadniczej nowelizacji projektowanej ustawy o zwalczaniu nadużyć w komunikacji elektronicznej (która wejdzie w życie przed regulacjami związanymi z wdrożeniem EKŁE). Niniejsze potwierdza konieczność ponownego rozważenia zasadności regulowania kwestii nadużyć w komunikacji elektronicznej odrębnym aktem normatywnym funkcjonującym obok ustaw „głównych”.  Zauważyć ponadto należy, że w uzasadnieniu do przedstawionego projektu ustawy Projektodawca podkreśla, że „*kwestia zwalczania nadużyć nie jest regulowana w Europejskim Kodeksie Łączności Elektronicznej oraz nie była dotychczas regulowana w ustawie – Prawo telekomunikacyjne*”.  Zważywszy na powyższe wskazać jednak w tym miejscu należy, że:  1) przepis art. 2 pkt 26 projektu *ustawy - Prawo komunikacji elektronicznej* wprowadza  pojęcie „*nadużycia telekomunikacyjnego*”, do którego następnie odnosi się m.in. art. 343 tego projektu ustawy, który *nota bene* wdraża art. 97 ust. 2 dyrektywy Parlamentu Europejskiego  i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej, dalej jako „EKŁE”;  2) kontrola działalności polegającej na zapewnianiu komunikacji elektronicznej jest przedmiotem projektowanej ustawy – Prawo komunikacji elektronicznej;  3) niektóre pojęcia, które Projektodawca wprowadził do przedstawionego projektu ustawy należą do terminologii którą operuje EKŁE i które w tabeli zgodności projektu *ustawy – Prawo komunikacji elektronicznej* wskazane są jako wdrażające przepisy EKŁE. Wskazać tu należy pojęcia definiowane w art. 2 pkt 12 i 13 przedmiotowego projektu – „usługa komunikacji interpersonalnej” oraz „usługa komunikacji interpersonalnej niewykorzystująca numerów” – w EKŁE odpowiednio „usługa łączności interpersonalnej” i „usługa łączności interpersonalnej niewykorzystująca numerów” (art. 5 pkt 5 i 7 EKŁE).  Przedmiotowy projekt nie zawiera jednak odnośnika europejskiego informującego o wdrażaniu postanowień aktu normatywnego ustanowionego przez instytucję Unii Europejskiej, o którym mowa w § 19a ust. 1 Zasad techniki prawodawczej.  Mając powyższe na uwadze ponownego przeanalizowania i wyjaśnienia wymagają następujące kwestie:  1) czy koniecznym jest regulowanie przedmiotu opiniowanego projektu ustawy odrębną regulacją, a nie przygotowanie nowelizacji obowiązujących przepisów;  2) w przypadku potwierdzenia potrzeby odrębnej regulacji, o której mowa w pkt 1 – rozważenia wymaga, do której ustawy „głównej” przedmiotowy projekt ma się odnosić - do ustawy - Prawo telekomunikacyjne, czy do projektowanej ustawy – Prawo komunikacji elektronicznej (i czy w tym przypadku nie jest wskazane skorelowanie terminu wejścia  w życie przedmiotowego projektu z terminem wejścia w życie projektu *ustawy – Prawo komunikacji elektronicznej)*;  3) czy przedmiotowy projekt wdraża przepisy europejskie, a jeżeli tak, uzupełnienia dokumentacji projektu o dokumenty, o których mowa w § 30 Regulaminu pracy Rady Ministrów.  Powyższe informacje powinny zostać uwzględnione w uzasadnieniu przedmiotowego projektu, w jego części ogólnej. | **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). Art. 97 ust. 2 EKŁE odnosi się do obowiązku zapewnienia przez państwo członkowskie, aby właściwe organ/organ 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 art. 343, który również zostanie „przeniesiony” do projektowanej ustawy o zwalczaniu nadużyć w komunikacji elektronicznej w zakresie w jakim Prezes UKE może nakazać przedsiębiorcy telekomunikacyjnemu zablokowanie dostępu do numeru lub usługi oraz nałożyć obowiązek wstrzymania pobierania opłat za połączenia lub usługi zrealizowane po upływie tego terminu, gdy jest to uzasadnione ochroną użytkowników końcowych przed nadużyciami w komunikacji elektronicznej  Ze względów formalnych projekt musi się odnosić do obecnie obowiązujących przepisów, tj. ustawy – Prawo telekomunikacyjne, natomiast projektodawca ma świadomość zaawansowanych prac nad nową ustawą zastępującą ustawę -Prawo telekomunikacyjne, tj. projektem ustawy - Prawo komunikacji elektronicznej.  Po analizie uwag RCL oraz MSUE wskazujemy, że przedmiotowy projekt wdraża przepisy europejskie (art. 97 ust. 2 EKŁE) i równocześnie zostanie uzupełniona dokumentacja o dokumenty, o których mowa w § 30 - Regulaminu pracy Rady Ministrów.  Ponadto, zgodnie ze wskazaniem RCL, zostało uzupełnione uzasadnienie. |
|  | | RCL | Tytuł ustawy | z przepisu art. 1, a także z kolejnych przepisów przedstawionego projektu ustawy wynika, że projekt ten reguluje kwestie zarówno zwalczania nadużyć w komunikacji elektronicznej jak i zapobiegania tym nadużyciom. Wobec powyższego, mając na uwadze § 18 Zasad techniki prawodawczej, zgodnie z którym przedmiot ustawy określa się możliwie najzwięźlej, jednakże w sposób adekwatnie informujący o jej treści, proponuje się rozważenie zmiany przedmiotu ustawy w tytule przez jego uzupełnienie o element „zapobiegania” nadużyciom, bądź uogólnienie tego przedmiotu ustawy przez nadanie mu brzmienia „o nadużyciach w komunikacji elektronicznej”; | **Uwaga wyjaśniona**  Przepisy ustawy rozróżniają pojęcia „zapobieganie” oraz „zwalczanie”, biorąc pod uwagę, że przepisy te zawierają rozwiązania zarówno o charakterze prewencyjnym (zapobiegawczym, zmniejszającym występowanie negatywnego zjawiska nadużyć), jak i następczym. O ile rozróżnienie tych terminów na gruncie poszczególnych norm prawnych jest uzasadnione, o tyle obecny tytuł ustawy odnoszący się do zwalczania nadużyć w komunikacji elektronicznej jest zarazem możliwie jak najbardziej zwięzły, jednocześnie oddaje odpowiednio precyzyjnie przedmiot regulacji. |
|  | | RCL | Art. 2 pkt 2 | zgodnie z art. 2 pkt 2 projektu dostawcą poczty elektronicznej jest osoba fizyczna, osoba prawna albo jednostka organizacyjna nieposiadająca osobowości prawnej, która prowadząc, chociażby ubocznie, działalność zarobkową lub zawodową świadczy usługę poczty elektronicznej. Zauważyć jednak należy, że przedmiotowy projekt nie definiuje „usługi poczty elektronicznej”, a jedynie „pocztę elektroniczną”, co wymaga niezbędnej korekty; | **Uwaga uwzględniona** Przy definicji „dostawcy poczty elektronicznej” usuwa się zbędne słowo „usługę”, gdyż „poczta elektroniczna” jest definiowana jako „usługa”.  Przepis zostanie przeredagowany. |
|  | | RCL | Art. 2 pkt 3 | w przypadku definicji zawartej w art. 2 pkt 3 projektu, dotyczącej „komunikatu elektronicznego”, zauważyć należy, że definicja ta pokrywa się z definicją „komunikatu” zawartą w ustawie – Prawo telekomunikacyjne (art. 2 pkt 17), uzupełnioną jedynie o element „usług komunikacji interpersonalnej niewykorzystujących numerów”. Mając na uwadze przepis § 9 Zasad techniki prawodawczej, zgodnie z którym w ustawie należy się posługiwać określeniami, które zostały użyte w ustawie podstawowej dla danej dziedziny spraw, w szczególności w ustawie określanej jako „kodeks” lub „prawo”, definicja „komunikatu elektronicznego” wymaga przeredagowania, przez odesłanie do definicji zawartej w ustawie – Prawo telekomunikacyjne; | **Uwaga uwzględniona**  Odesłanie zostanie zmienione na odesłanie do definicji „komunikatu”, o której mowa w ustawie Prawo telekomunikacyjne. |
|  | | MS | Art. 2 pkt 3 | Wątpliwości budzi wprowadzenie do projektu nowej definicji komunikatu elektronicznego (art. 2 pkt 3), w sytuacji, gdy już taka definicja znajduje się w ustawie z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz. U. z 2021 r. poz. 576, z późn. zm.). Nowa definicja ma się różnić od obecnej i być rozszerzona o pojęcie dotyczące informacji przekazywanych za pośrednictwem publicznie dostępnych usług komunikacji elektronicznej, a nie jak dotychczas jedynie publicznie dostępnych usług telekomunikacyjnych. Należałoby zatem w tym zakresie dokonać rozszerzenia definicji komunikatu elektronicznego zawartego w Prawie telekomunikacyjnym, a w projekcie ustawy jedynie odwołać się do tej definicji. Nie ma bowiem potrzeby wprowadzenia dwóch definicji legalnych tego samego pojęcia de facto w tej samej dziedzinie prawa. | **Uwaga uwzględniona**  Odesłanie zostanie zmienione na odesłanie do definicji „komunikatu”, o której mowa w ustawie - Prawo telekomunikacyjne. |
|  | | RCL | Art. 2 pkt 4 | odnosząc się do definicji „nadużycia w komunikacji elektronicznej” zawartej w art. 2 pkt 4 projektu – zauważenia wymaga, że treść tej definicji tożsama jest z projektowanym brzmieniem definicji „nadużycia telekomunikacyjnego” zawartego w projekcie ustawy - Prawo komunikacji elektronicznej. Tym samym wyjaśnienia wymaga zastosowanie w przypadku przedmiotowego projektu terminologii „*nadużycia w komunikacji elektronicznej*” (w miejsce nadużycia „*telekomunikacyjnego*”) definiując je jednocześnie jako świadczenie usługi telekomunikacyjnej lub korzystanie z urządzeń telekomunikacyjnych; | **Uwaga wyjaśniona**  Kwestie dotyczące nadużyć telekomunikacyjnych w projekcie ustawy - Prawo komunikacji elektronicznej zostaną usunięte. Ustawa nakłada również obowiązki na dostawcę poczty elektronicznej, który nie jest przedsiębiorcą telekomunikacyjnych i nie świadczy usługi telekomunikacyjnej, ale świadczy usługę komunikacji elektronicznej. |
|  | | RCL | Art. 2 pkt 8 | mając na uwadze funkcjonujące w systemie prawa jako jeden ze środków komunikacji elektronicznej (o których mowa w ustawie z dnia 18 lipca 2002 r. o świadczeniu usług drogą elektroniczną), bez konieczności dodatkowego ustawowego definiowania, pojęcie „poczty elektronicznej”, dodatkowego wyjaśnienia wymaga przyczyna wprowadzenia takiej definicji w art. 2 pkt 8 projektu. Ponadto zauważyć należy, że przedmiotowa definicja „poczty elektronicznej” zawiera dane techniczne dotyczące przekazywania komunikatu elektronicznego (standard SMPT, POP3, IMAP4) które, powinny zostać z projektu usunięte ze względu na ich zbyt techniczny i specjalistyczny charakter, a także możliwość częstych nowelizacji przyszłej regulacji ze względu na postęp technologiczny. | **Uwaga wyjaśniona** Standard SMTP, który opisał Jonathan Postel w dokumencie RFC 821 około 40 lat temu jest nadal stosowany.  Jednocześnie, odniesienie do tych standardów technicznych jest niezbędne aby odróżnić usługę poczty elektronicznej od innych usług interpersonalnych niewykorzystujących numerów (jak np. tzw. komunikatory internetowe), gdyż ustawa o świadczeniu usług drogą elektroniczną nie zawiera legalnej definicji poczty elektronicznej. |
|  | | RCL | Art. 2 pkt 9 | w przypadku definicji „*połączenia głosowego*” określonej w art. 2 pkt 9 projektu – analogicznie jak w przypadku definicji „*komunikatu elektronicznego*” zauważyć należy, że powtarza ona definicję „*połączenia telefonicznego*”, o której mowa w art. 2 pkt 26 ustawy – Prawo telekomunikacyjne – zastępując w tej definicji „*publicznie dostępną usługę telekomunikacyjną*” – „*publicznie dostępną usługą komunikacji interpersonalnej*” czyli pojęciem z zakresu EKŁE, dotychczas nie wdrożonego do krajowego systemu prawa; na marginesie wskazać należy, że pojęcie „*połączenia głosowego*” zostało natomiast zdefiniowane w projekcie *ustawy – Prawo komunikacji elektronicznej,* co potwierdza jedynie konieczność dokonania ponownej analizy usytuowania systemowego przedmiotowego projektu i jego odniesienia się do odpowiedniej ustawy podstawowej. | **Uwaga wyjaśniona**  Jak słusznie wskazano w uwadze, definicje te różnią się, a ustawa Prawo komunikacji elektronicznej jest wciąż projektem aktu prawnego, dlatego zasadne jest pozostawienie definicji w obecnym brzmieniu. Jednocześnie możliwe jest właściwe odczytanie normy prawnej w odniesieniu do obecnego stanu prawnego. |
|  | | MON | Art. 3 ust. 1 | 1. W art. 3 w ust. 1 proponuje się uzupełnić katalog nadużyć o dodatkowe punkty 4 i 5, w następującym brzmieniu:   *„4) nieuprawnionego używania telekomunikacyjnych urządzeń końcowych i automatycznych systemów wywołujących do celów marketingu bezpośredniego lub przesyłania niezamówionej informacji handlowej, bez posiadania uprzedniej, bezpośredniej zgody abonenta lub użytkownika końcowego, o której mowa w art. 172 ust. 1 ustawy z dnia 16 lipca 2004 r. - Prawo telekomunikacyjne;*  *5) nieuprawnionego wykorzystania danych o lokalizacji urządzeń końcowych, wykraczających poza dane niezbędne do transmisji zamówionego komunikatu, o których mowa w art. 159 ust. 1 pkt 4 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne, w szczególności wykorzystania danych pochodzących z systemów sygnalizacji SS7 oraz adresów IP pozyskiwanych przy wykorzystaniu znaczników śledzących.”.*  Uzasadnieniem do rozszerzenia katalogu nadużyć jest coraz powszechniejsze zjawisko prób wyłudzenia danych pracowników instytucji rządowych pod pretekstem prowadzenia kampanii marketingowych oraz dodatkowo przeprowadzanie prób ustalenia aktualnych danych lokalizacyjnych tych osób.  W konsekwencji powyższej uwagi, proponuje się rozszerzyć katalog kar określonych w art. 15 i 16o uzupełnione formy wykroczeń (art. 3 ust. 1 pkt 4 i 5), z tym zastrzeżeniem, że w przypadku powtarzalności wykroczeń, o których mowa w art. 3 ust. 1 pkt 4 i 5 w stosunku do użytkowników rządowych oraz jednoczesnym wykroczeniu z art. 3 ust. 1 pkt 4 lub 5 w przypadku osób prywatnych - możliwą karą byłoby odcięcie sprawcy dostępu do publicznej sieci telekomunikacyjnej. Szczegółowe rozwiązania dotyczące kar za wykroczenia z art. 3 ust. 1 pkt 4 i 5 proponuję wypracować w toku dalszych prac nad projektowaną ustawą. | **Uwaga wyjaśniona**  Niedozwolony marketing bezpośredni i przesyłanie niezamówionej informacji handlowej może mieścić w szerokorozumianym zjawisku nadużyć w komunikacji elektronicznej, natomiast różni się od pozostałych nadużyć wskazanych wprost w projektowanej ustawie o zwalczaniu nadużyć w komunikacji elektronicznej. Biorąc pod uwagę, że zgodnie z założeniami ustawy to przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie, nie jest zasadne wyodrębnianie kolejnej kategorii nadużyć.  Uzasadnienie pozostaje aktualne w kontekście postulatu dodania nieuprawnionego wykorzystania danych o lokalizacji urządzeń końcowych, wykraczających poza dane niezbędne do transmisji zamówionego komunikatu, jako nadużycia telekomunikacyjnego.  Zasadne jest więc pozostawienie rzeczonej regulacji w ustawie Prawo telekomunikacyjne (i projektowanym Prawie komunikacji elektronicznej, zgodnie z wersją z 5 maja 2022 r. do tego zagadnienia odnosi się art. 393 projektu). |
|  | | MKSS | Art.3 | Zwracam również uwagę na przepisy regulujące kwestie zjawiska CLI *spoofingu*, rozumianego przez projektodawcę jako 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 połączenia do określonego działania (art. 3 ust. 1 pkt 3). Przepisy dotyczące zapobiegania i zwalczania CLI *spoofingu*, powinny zostać uzupełnione o kwestie regulujące ogólne zasady oraz warunki stosowania mechanizmu blokowania niechcianych połączeń telefonicznych, podobnie jak ma to miejsce w kontekście *smishingu* | **Uwaga wyjaśniona**  Szczegóły związane z tymi mechanizmy będą zawarte w porozumieniu z Prezesem UKE albo w rekomendacjach Prezesa UKE. |
|  | | MKSS | Art. 3 ust. 1 | Odnosząc się do zjawiska *smishingu*, rozumianego przez projektodawcę jako podszywanie się przez nadawcę pod inny podmiot w celu nakłonienia odbiorcy tej wiadomości do określonego działania (art. 3 ust. 1 pkt 2), należy zauważyć, że przedmiotowy projekt koncentruje się na zwalczaniu zjawiska *smishingu* zasadniczo wyłącznie w odniesieniu do usługi przesyłania krótkich wiadomości tekstowych (SMS), co zdecydowanie ogranicza efektywność zakładanej regulacji. Zasadne jest, aby projektowane rozwiązania obejmowały również usługę wiadomości multimedialnych (MMS) oraz najnowszy, wdrażany obecnie standard komunikacji mobilnej RCS. Jednocześnie, w celu zapewnienia zrozumiałości proponowanych przepisów, proponuję przeniesienie do art. 2 projektu definicji pojęcia „*smishing*”, jak i pozostałych, wymienionych w ustawie rodzajów działań mających cechy nadużyć, o których mowa w projektowanej ustawie (art. 3 ust. 1). | **Uwaga wyjaśniona**  W innych przepisach ustawy została uwzględniona kwestia przeciwdziałania nadużyciom w telekomunikacji dokonywanym za pomocą MMS. |
|  | | MRiT | Art. 3 ust. 2 | Dodatkowo Ministerstwo Rozwoju i Technologii zgłasza uwagę do art. 3 ust. 2 projektu, zgodnie z którym, na przedsiębiorcę telekomunikacyjnego nakłada się obowiązek podejmowania proporcjonalnych działań mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. MRiT z pełną aprobatą odnosi się do celu jaki ma realizować ten przepis. Niemniej zaproponowane brzmienie, może budzić wątpliwości. W opinii DDR, regulacja nakłada obowiązek na przedsiębiorców w zbyt ogólny sposób. Wśród adresatów mogą powstać wątpliwości, jakiego konkretnie działania wymaga się od nich w przypadku wystąpienia zjawisk nadużyć w komunikacji elektronicznej. Konsekwentnie może także powstać problem z wyegzekwowaniem tych obowiązków oraz nieuzasadnione poszerzenie zakresu działań czy kompetencji organu stosującego prawo.  Mając powyższe na uwadze, MRiT poddaje pod rozwagę, sformułowanie przedmiotowego przepisu w sposób bardziej precyzyjny. | **Uwaga wyjaśniona** Adresatem obowiązku z art. 3 ust. 2 projektu jak przesądza wprost przepis jest „przedsiębiorca telekomunikacyjny”.  Nadużycia w komunikacji elektronicznej mają 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 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 w telekomunikacji, komunikacji elektronicznej. |
|  | | MS | Art. 3 ust. 2 | W projektowanym art. 3 ust. 2 zawarto regulację, zgodnie z którą przedsiębiorca telekomunikacyjny będzie obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Kolejne przepisy projektu ustawy nie zawierają jednak regulacji, umożliwiających wykładnię przywołanego zwrotu, co może potem rodzić wątpliwości interpretacyjne. Uzasadnienie do projektu ustawy również nie zawiera wyjaśnienia tej kwestii. Należy również wskazać na brak regulacji w zakresie procedur odwoławczych w przypadku zastosowania tego rodzaju środków przez przedsiębiorcę telekomunikacyjnego. | **Uwaga wyjaśniona**  Środki mające na celu zapobieganie nadużyciom mają być proporcjonalne – uwzględniające możliwości podmiotu w zakresie podejmowania działań, a 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. W tym zakresie uzasadnienie zostało uzupełnione. |
|  | | RCL | Art. 3 ust. 2 | odnośnie do art. 3 ust. 2 projektu, wyjaśnienia wymaga, czy do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie obowiązany jest także dostawca poczty elektronicznej oraz podmiot publiczny (o którym mowa w art. 2 pkt 6 projektu), na których projekt ustawy także nakłada obowiązki związane z zapobieganiem nadużyciom w komunikacji elektronicznej. Ponadto wskazać należy, że przepis ust. 2 ma charakter niedookreślony i wymaga uzupełnienia o wskazanie punktu odniesienia do ustalenia „proporcjonalnych” środków technicznych i organizacyjnych – jak np. wielkość przedsiębiorcy, obrót, cel, wysokość przychodów w danym roku kalendarzowym. Zwrócić także należy uwagę na konieczność ustalenia chociażby minimalnego poziomu środków technicznych i organizacyjnych których stosowanie byłoby obowiązkiem przedsiębiorcy, w przeciwnym wypadku mamy do czynienia z nałożeniem obowiązku o bliżej niesprecyzowanym charakterze. | **Uwaga wyjaśniona** Adresatem obowiązku z art. 3 ust. 2 projektu jak przesądza wprost przepis jest „przedsiębiorca telekomunikacyjny”.  Nadużycia w komunikacji elektronicznej mają 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 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 zakresie punktu odniesienia uzupełnione zostało uzasadnienie ustawy. |
|  | | MKSS | Art. 3 ust. 2 | Pragnę zwrócić uwagę na art. 3 ust. 2 projektu, w myśl którego przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Norma wyrażona tym przepisem została sformułowana w sposób nieprecyzyjny i ocenny. Nakłada ona obowiązki na przedsiębiorcę telekomunikacyjnego, ale jednocześnie nie można jednoznacznie stwierdzić jakie działania stanowią wypełnienie ww. normy. W związku z tym wydaje się, iż przepis ten powinien zostać usunięty albo doprecyzowany. | **Uwaga wyjaśniona**  Nadużycia w komunikacji elektronicznej mają 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 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 w telekomunikacji, komunikacji elektronicznej. |
|  | | MS | Art. 4 ust. 1 | **3.** Wątpliwy jest też przepis **art. 4 ust. 1** projektu, zgodnie z którym Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT NASK) na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie *smishingu*, czyli działania polegającego na wyłudzeniu danych osobowych za pośrednictwem SMS. Norma ta uprawnia CSIRT NASK do monitorowania występowania *smishingu* bez określenia trybu tego monitoringu i jego zakresu, w tym zakresu dostępu, zakresu podlegających kontroli danych, podmiotów które będą podlegać monitoringowi. W tej części sposób monitorowania występowania tego zjawiska powinien być ściśle uregulowany w ustawie przez określenie trybu monitorowania tego nadużycia oraz jego kontroli. Przekazanie nieograniczonych uprawnień do monitorowania nadużyć daje też nieograniczone uprawnienia do wglądu do systemów informatycznych firm telekomunikacyjnych, jak też na konta osób fizycznych, i może się wiązać z naruszeniem interesów tajemnicy przedsiębiorstwa, jego interesów gospodarczych, czy też wolności komunikowania się. | **Uwaga wyjaśniona**  CSIRT NASK będzie monitorował występowanie zjawiska smishingu na podstawie danych przekazanych mu przez podmioty trzecie – odbiorców SMS czy np. samych przedsiębiorców telekomunikacyjnych. Będzie to się odbywało dokładnie w taki sam sposób jak to się dzieje obecnie – poprzez przekazanie sms na specjalny numer[[1]](#footnote-2) albo poprzez formularz na stronie internetowej[[2]](#footnote-3). Niniejszy projekt ustawy nie przyznaje CSIRT NASK uprawnienia do np. żądania informacji stanowiących tajemnicę przedsiębiorstwa w celu monitorowania smishingu. |
|  | | MKSS | Art. 4 ust. 1 | Ponadto, w projektowanym art. 4 ust. 1 projektu zawarto rozwiązanie, zgodnie z którym CSIRT NASK monitoruje występowanie smishingu na podstawie informacji otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS). CSIRT NASK powinien inicjować monitoring zjawiska smishingu także na podstawie pozostałych działań, np. posiadanej wiedzy własnej, a także występowania doniesień medialnych. | **Uwaga wyjaśniona**  Ustawa określa jedynie podstawowy sposób otrzymywania przez CSIRT NASK informacji o nadużyciach w komunikacji elektronicznej. Nie oznacza to, że będą to jedyne źródła – CSIRT NASK,  CSIRT NASK będzie prowadził monitoring zjawiska smishingu także na podstawie pozostałych działań, np. posiadanej wiedzy własnej, a także występowania doniesień medialnych. |
|  | | RCL | Art. 4 ust. 1 | w przypadku projektowanego art. 4:  a) zauważyć należy brak chociażby podstawowego uregulowania procedury zgłaszania przez odbiorcę „wystąpienia smishingu” – wydaje się bowiem, że regulacja ust. 1 wskazująca na „otrzymane od odbiorców krótkie wiadomości tekstowe (SMS)” są niewystarczającą  regulacją proceduralną. Nie wiadomo bowiem, czy odbiorca przekazuje treść otrzymanej od nadawcy wiadomości, czy wysyła odrębne zgłoszenie podejrzenia nadużycia. Nie wiadomo także gdzie takie zgłoszenie może być przekazywane (z projektu wynika jedynie, że CSIRT NASK otrzymuje od odbiorców krótkie wiadomości), ani jakie dane przekazuje się łącznie z tą wiadomością, | **Uwaga wyjaśniona**  Odbiorca może przesłać treść podejrzanej wiadomości wraz ze wskazaniem numeru. Przekazanie będzie mogło się odbyć poprzez przesłanie takiej wiadomości sms’em do CSIRT NASK  albo poprzez formularz na stronie internetowej. O informacje w tym zakresie zostanie uzupełnione uzasadnienie do ustawy. |
|  | | RCL | Art. 4 ust. 1 | b) wskazać należy, że zadania CSIRT NASK regulują przepisy ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (art. 26 ust. 1, 3 i 6 tej ustawy) - nie wymienia ona jednak, wśród zadań CSIRT NASK, zadań CSIRT NASK powierzonych temu podmiotowi na podstawie przedmiotowego projektu ustawy. Przedmiotowy projekt nie zawiera także przepisów zmieniających ww. ustawę w zakresie powierzenia CSIRT NASK nowych zadań, co wymaga uzupełnienia, | **Uwaga uwzględniona**  Wprowadzono przepisy zmieniające ustawę o krajowym systemie cyberbezpieczeństwa w zakresie odnoszącym się do zadań CSIRT NASK. |
|  | | RCL | Art. 4 | c) wyjaśnienia, a następnie ewentualnego doregulowania w projekcie, wymagają następujące kwestie:  - kim jest „odbiorca” wskazany w ust. 1, i czy każdy kto otrzymał wiadomość tekstową co do której ma podejrzenie występowania smishingu może ją zgłosić do CSIRT NASK i w jaki sposób,  - na czym polega „monitorowanie” występowania smishingu – czy informacje/wiadomości od odbiorców będą gromadzone, przetwarzane i w jakim miejscu będą one przetwarzane (czy chodzi o system teleinformatyczny, o którym mowa w ust. 3?),  - kto odpowiada za funkcjonowanie systemu teleinformatycznego, o którym mowa w ust. 3, kto jest jego administratorem i administratorem danych w nim gromadzonych (o ile są gromadzone), jakie dane/informacje będą w nim gromadzone i przetwarzane, jak długo będą w tym systemie przechowywane – po jakim czasie się je usuwa i czy w systemie tym przetwarza się także dane osobowe,  - czy „wzorcem wiadomości wyczerpującej znamiona smishingu” jest jedynie treść takiej wiadomości, czy jest to także jej forma – zauważyć bowiem należy, że zgodnie z ust. 6 pkt 1 przedsiębiorca telekomunikacyjny obowiązany jest do blokowania krótkich wiadomości tekstowych zawierających treści zawarte we wzorcu, a nie zgodnie z wzorcem. We wskazanym zakresie przedmiotowy projekt wymaga uspójnienia pojęć,  - jaki charakter będą miały rozstrzygnięcia podejmowane przez CSIRT NASK dotyczące uznania, bądź nie uznania danej wiadomości za smishing, a niosące za sobą konsekwencje blokowania wysyłania danych (automatycznego). Zauważyć należy, że na skutek „decyzji” CSIRT NASK może zostać ograniczona możliwość prowadzenia działalności przez podmioty będące nadawcami takich wiadomości, a które, co wynika z projektowanych przepisów nie zostaną powiadomione o zgłoszeniu i „decyzji” o zablokowaniu przesyłanych przez nie wiadomości. Nie wiadomo także w jakich okolicznościach i w jakiej formie prowadzone będzie przez CSIRT NASK „postępowanie” w sprawie uznania, że zablokowana treść nie stanowi smishingu albo dalsze blokowanie tych wiadomości jest niecelowe. Nie wiadomo także jakie mają być przesłanki dla zamiany decyzji CSIRT NASK we wskazanym wcześniej zakresie wznowienia „postępowania”. Wydaje się, że w tej kwestii projekt wymaga odpowiedniego uzupełnienia,  - w jaki sposób przedsiębiorcy telekomunikacyjni będą mieli zapewniony dostęp do systemu teleinformatycznego, o którym mowa w ust. 3,  - czy do systemu, o którym mowa w ust. 3, trafia tylko wzorzec wiadomości/treść zawarta we wzorcu, czy także informacje dotyczące np. numeru, z którego taka wiadomość jest nadawana, a konsekwentnie – czy blokowane, zgodnie z ust. 6 pkt 1, są wiadomości zawierające określoną treść wskazaną we wzorcu, czy także wiadomości wysyłane z danego numeru,  - cel dla jakiego CSIRT NASK udostępnia na swojej stronie internetowej wzorzec wiadomości wyczerpującej znamiona smishingu. Jeżeli, jak się wydaje, zamieszczanie takiej informacji pełni funkcje informacyjne i ostrzegawcze dla użytkowników – wyjaśnienia wymaga długi 14, a nawet 21-dniowy termin na zamieszczenie takiego ostrzeżenia,  - czy o uznaniu wiadomości za wyczerpującą znamiona smishingu, a następnie przekazaniu tej informacji w systemie teleinformatycznym, o którym mowa w ust. 3, w celu blokowania tych wiadomości, CSIRT NASK informuje nadawcę tej wiadomości, tak aby miał możliwość niezwłocznego wniesienia sprzeciwu, o którym mowa w art. 5, | **Uwaga wyjaśniona**  Ze względu na ciągłe rozbudowanie możliwości co do zgłaszania incydentów, w tym podejrzanych sms’ów do CSIRT NASK, w celu dotarcia do ogółu społeczeństwa, nie jest zasadne przesądzanie (doregulowywanie) tych kwestii na poziomie ustawy. Aktualne sposoby zgłaszania zostaną uzupełnione w uzasadnieniu.  Celem nie jest pozbawienie nikogo możliwości zgłaszania podejrzanych wiadomości do CSIRT NASK, dlatego zapewnia się, że każdy kto otrzymał wiadomość tekstową co do której ma podejrzenie występowania smishingu może ją zgłosić do CSIRT NASK.  „Monitorowanie” ma takie znaczenie jak w języku powszechnym, prawnym i prawniczym.  Zamieszczenie na stronie internetowej wzorców wiadomości wyczerpującej znamiona smishingu ma na celu zapewnienie transparentności działania CSIRT NASK oraz funkcję informacyjną dla nadawców wiadomości o danym wzorze, a także wspierają instytucję sprzeciwu. Publikowanie wzorców nie pełni funkcji ostrzegawczej dla użytkowników (wiadomości zgodne ze wzorcem do nich nie trafiły i nie będą trafiać), w rozumieniu jaki wskazuje RCL.  Jednocześnie natychmiastowa czy bardzo szybka publikacja wzorców przez NASK powodowałaby natychmiastowe dostosowanie przez nadawców oszukańczych wiadomości (zmiana wzorca smishingowego przez nadawcę aby nie podlegał on blokowaniu). |
|  | | MS | Art. 4 ust. 3 | Ponadto w art. 4 ust. 3projektu został sformułowany obowiązek CSIRT NASK przekazania za pośrednictwem systemu teleinformatycznego, m.in. Komendantowi Głównemu Policji, informacji o wystąpieniu *smishingu* wraz z wzorcem wiadomości wyczerpującej jego znamiona. Należy zauważyć, że będzie to automatycznie wiązało się z koniecznością wszczęcia postępowania o czyn ścigany z urzędu. Mając na względzie ilość nazw domenowych wpisywanych dziennie na listę ostrzeżeń, prowadzoną przez NASK, będzie to generowało od kilkunastu do kilkudziesięciu nowych postępowań przygotowawczych dziennie. | **Uwaga wyjaśniona**  Projektodawca zakłada, że dostęp do wiedzy o występowaniu smishingu pozwoli Policji (a w szczególności Centralnemu Biuru Zwalczania Cyberprzestępczości) na skuteczniejsze zwalczanie tego typu przestępstw. Część wiadomości może pochodzić od tych samych oszustów. Należy podkreślić, że te czyny już dziś są penalizowane i powinny być zgłaszane w przypadku wykrycia zarówno przez użytkowników jak i przedsiębiorców. |
|  | | MKSS | Art. 4 ust. 4 | Należy także zauważyć, że w projektowanym art. 4 ust. 4 ustawy określono 14-dniowy termin (maksymalnie 21-dniowy), w jakim CSIRT NASK będzie zobowiązany upublicznić na swojej stronie internetowej wzorzec wiadomości wyczerpujący znamiona *smishingu*. Wzorce wiadomości ww. rodzaju powinny być przekazywane do publicznej informacji niezwłocznie, równolegle z informowaniem podmiotów wskazanych w projektowanym art. 4 ust. 3 ustawy. Charakter kampanii *smishingowych* sprawia, iż często są one krótkotrwałe, a jednocześnie bardzo intensywne, przez co szczególnie 21-dniowy termin może się okazać niewystarczający do odpowiedniego uświadomienia społeczeństwa o zakresie występujących zagrożeń. W związku z powyższym proponuje się zastąpienie w projektowanym art. 4 ust. 4 ustawy zwrotu „w terminie 14 dni nie później jednak niż w terminie 21 dni wyrażeniem „niezwłocznie, nie później jednak niż w terminie 14 dni” | **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 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 zmienić stosowane przez nich wiadomości i mogłoby to sprawić, że ustawa nie zrealizuje swojego celu. |
|  | | RCL | Art. 4 ust. 5 | d) mając na uwadze, że CSIRT NASK zgodnie z przepisem ust. 5 może uznać, że treść zawarta we wzorcu wiadomości nie stanowi smishingu proponuje się rozważenie uzupełnienia przepisu ust. 3 o wskazanie, że chodzi o informację o podejrzeniu wystąpienia smishingu. Powyższe wskazuje jednak na dodatkowy problem – czy na podstawie jedynie tylko podejrzenia, że wiadomość wyczerpuje znamiona smishingu, CSIRT NASK powinien informować o tym przedsiębiorców telekomunikacyjnych i powodować tym samym natychmiastowe zablokowanie wysyłania wiadomości? Z projektowanych przepisów wynika bowiem, że CSIRT NASK może w dowolnym terminie zmienić kwalifikację danej wiadomości, uznanej uprzednio za smishing, umożliwiając nadawcy jej dalsze rozsyłanie (o tym fakcie, jak wynika z projektu, także nie informuje nadawcy). W powyższym zakresie proponuje się ponowne przeanalizowanie projektowanej regulacji pod kątem doprecyzowania, kiedy i na podstawie jakich przesłanek CSIRT NASK podejmuje decyzję o zablokowaniu wiadomości, bądź ich odblokowaniu, | **Uwaga wyjaśniona**  To CSIRT NASK ma dokonywać merytorycznej kwalifikacji niezbędnej do późniejszego blokowania wiadomości, nie jest więc zasadne, aby przekazywał informacje „o podejrzeniu wystąpienia smishingu” i to bez dookreślenia skutków z jakimi wiązałoby się przekazanie samego „podejrzenia”. Dlatego rozwiązanie zaproponowane przez RCL jest w ocenie projektodawcy niewłaściwe.  Smishing jest zdefiniowany i przesłanki kwalifikacji są dostatecznie doprecyzowane (dotyczy to sytuacji gdy 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). Możliwa jest zmiana kwalifikacji w trybie swoistej samokontroli.  Niemniej, ponowna analiza zagadnień wskazanych przez RCL, wskazuje, że należy przesądzić, co dzieje się z udostępnionymi na stronie wzorcami, w sytuacji, gdy wiadomość (wzorzec) jednak nie nosi znamion smishingu lub niecelowe jest dalsze blokowanie wg tego wzorca. |
|  | | RCL | Art. 4 ust. 6 pkt 2 | e) w przypadku ust. 6 pkt 2 proponuje się doprecyzowanie obowiązku zaprzestania blokowania wiadomości tekstowych przez wskazanie, że przedsiębiorca telekomunikacyjny również ten obowiązek wykonuje niezwłocznie; | **Uwaga uwzględniona** |
|  | | RCL | Art. 5 ust. 2-4 | 9) w przypadku art. 5 ust. 2-4 projektowanej ustawy wyjaśnienia wymaga, czy sprzeciw wnoszony przez nadawcę wiadomości, oprócz uzasadnienia i wskazania numeru wykorzystywanego do nadania wiadomości, nie powinien również zawierać danych identyfikacyjnych nadawcy;  wskazać należy także, że Projektodawca nie przewidział procedury prowadzącej do uzupełnienia sprzeciwu w przypadku braków formalnych – w takiej sytuacji wydaje się właściwym rozważenie wprowadzenia przepisu wprowadzającego obowiązek Prezesa UKE do wezwania nadawcy wnoszącego sprzeciw do uzupełnienia braków w wyznaczonym terminie pod rygorem pozostawienia sprzeciwu bez rozpoznania; | **Uwaga uwzględniona**  w zakresie uzupełnienia, że sprzeciw zawiera dane identyfikujące nadawcę, w szczególności  a) imię i nazwisko, adres zamieszkania - w przypadku osób fizycznych,  b) nazwę podmiotu, adres, numer z właściwego rejestru - w przypadku osób prawnych.  **Uwaga wyjaśniona**  w zakresie wymogu wezwania do uzupełnienia sprzeciwu jako działania nieadekwatnego i nieproporcjonalnego. Możliwe jest ponowienie sprzeciwu poprzez złożenie prawidłowego, tj. spełniającego wymogi formalne. Tryby szczególne procedur administracyjnych przewidują rozwiązania o takim charakterze. |
|  | RCL | | Art. 6 ust. 1 | zgodnie z art. 6 ust. 1 projektu Prezes UKE rozpatruje sprzeciw i informuje nadawcę o sposobie jego rozpatrzenia. Z przepisu ust. 2 wynika, że Prezes UKE może sprzeciw uwzględnić – brak jednak regulacji wskazującej na drugi sposób rozstrzygnięcia – nieuwzględniający sprzeciwu oraz określenia procedury odwoławczej od tego rozstrzygnięcia.  Wskazać także należy, że projektowane przepisy nie określają trybu w jakim Prezes UKE uwzględnia sprzeciw bądź go nie uwzględnia, nie wiadomo także czy Prezes UKE wydaje w tej sprawie decyzje. Ponadto zauważenia wymaga, analogicznie jak w przypadku CSIRT NASK, że zadania Prezesa UKE określone w art. 5 i art. 6 projektu ustawy nie znajdują odzwierciedlenia w zakresie działania Prezesa UKE, określonego w art. 192 ustawy – Prawo telekomunikacyjne, co wymaga wprowadzenia do przedmiotowego projektu odpowiednich przepisów zmieniających ww. ustawę; | **Uwaga uwzględniona** w zakresie uzupełnienia sposobów rozpatrzenia sprzeciwu wraz z określeniem przesłanek oraz uzupełnienia katalogu z art. 192 ustawy - Prawo telekomunikacyjne.  **Uwagi wyjaśnione w pozostałym zakresie.** 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. |
|  | RCL | | Art. 7 | 11) w przypadku art. 7 projektu, wprowadzającego możliwość dodatkowego, uznaniowego blokowania przez przedsiębiorcę telekomunikacyjnego wiadomości zawierających treści wyczerpujących znamiona smishingu, innych niż te określone we wzorcu  przygotowanym przez CSIRT NASK, wskazać należy że projektowana regulacja wymaga uzupełnienia o przepisy określające postępowanie prowadzące do zablokowania wiadomości, kwestie związane z ewentualnymi sprzeciwami (procedura odwoławcza), kwestie związane  z informowaniem CSIRT NASK, Prezesa UKE, Komendanta Głównego Policji oraz innych przedsiębiorców o wprowadzonej blokadzie. Wyjaśnienia także wymaga, w jakiej sytuacji przedsiębiorca może samodzielnie podjąć decyzję o zablokowaniu wiadomości –  uzasadnienie projektu w tym zakresie nie zawiera odpowiedniego wyjaśnienia. Wyjaśnienia także wymaga, dlaczego Projektodawca nie wprowadził do projektu obowiązku zgłaszania do CSIRT NASK bądź Prezesa UKE przypadków wiadomości wyczerpujących znamiona smishingu także przez przedsiębiorców telekomunikacyjnych, co mogłoby skutkować uwzględnieniem treści zawartych w tych wiadomościach we wzorcu, o którym mowa w art. 4 ust. 2; | **Uwaga częściowo uwzględniona**  w zakresie dodania do projektowanego art. 4 ust. 1 przedsiębiorcy telekomunikacyjnego jako podmiotu, od którego mogą pochodzić informacje o występowaniu smishingu.  **wyjaśniając pozostałe kwestie należy wskazać, że** zgodnie z art. 3 ust. 2 przedsiębiorca telekomunikacyjny jest obowiązany do podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie. Z tego względu konieczne jest również nadanie uprawnienia do blokowania sms’ów zawierających treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości, o którym mowa w art. 4 ust. 3, za pomocą systemu teleinformatycznego pozwalającego na automatyczną identyfikację takich krótkich wiadomości tekstowych (SMS) oraz wiadomości MMS.  Biorąc pod uwagę praktykę funkcjonowania rynku telekomunikacyjnego, takie działania mogą powodować odpowiedzialność kontraktową, więc nie jest uzasadnione wprowadzenie szczegółowej regulacji, o której mowa w uwadze. |
|  | MKSS | | Art. 7 | Dodatkowo należy zwrócić uwagę, że w projektowanym art. 7 zawarto rozwiązanie pozwalające operatorowi telekomunikacyjnemu na blokowanie krótkich wiadomości tekstowych (SMS) zawierających znamiona *smishingu*, innych niż te zawarte we wzorcu wiadomości sporządzonym przez CSIRT NASK. We wskazanej jednostce redakcyjnej nie zawarto jednak mechanizmu kontrolnego oraz odwoławczego, tj. rozwiązań analogicznych w stosunku do działań podejmowanych przez CSIRT NASK, w przypadku uznania danej wiadomości za *smishing*. Z tego powodu, w celu uspójnienia tworzonych regulacji w zakresie kwestii kontrolnych i odwoławczych, proponuję uzupełnienie przepisów we wskazanym zakresie. | **Uwaga wyjaśniona**  W przypadku zablokowania sprzeciwu na podst. art. 7 użytkownik końcowy będzie mógł skorzystać z reklamacji na ogólnych zasadach. |
|  | RCL | | Art. 8 | odnosząc się do projektowanego art. 8 także należy wskazać, że nakładając obowiązek blokowania połączenia głosowego bądź ukrywania identyfikacji numeru wywołującego Projektodawca nie określił procedury podejmowania takiej decyzji przez przedsiębiorcę telekomunikacyjnego, nie wskazał, w jakich okolicznościach i przypadkach numery są blokowane, a w jakich ukrywa się identyfikację numeru, czy od podjętej decyzji podmiot, którego numer zablokowano, może się odwołać, czy jest zawiadamiany o podjętych rozstrzygnięciach, a także, czy informacje o zablokowanych numerach trafiają do systemu teleinformatycznego, do którego dostęp mają podmioty wskazane w art. 4 ust. 3 projektu; | **Uwaga wyjaśniona**  Blokowanie połączenia głosowego jako środka dalej idącego od ukrycia identyfikacji numeru wywołującego dla użytkownika końcowego, powinno być stosowane, kiedy prawdopodobieństwo, że dochodzi do spoofingu jest bardzo wysokie lub wysokie. W pozostałych przypadkach przedsiębiorca telekomunikacyjny powinien ukryć identyfikację numeru wywołującego dla użytkownika końcowego.  Z definicji CLI Spoofing wynika, że jest to nieuprawnione posłużenie się przez użytkownika wywołującego połączenie głosowe informacją adresową wskazującą na osobę lub jednostkę organizacyjną inną niż ten użytkownik, więc nie jest celowe ani nie wydaje się proporcjonalne nakładanie obowiązku informacyjnego wobec dysponenta numeru. Nie dotyczy więc to „blokowania numerów” jak jest wskazane w uwadze, a blokowania „połączeń głosowych”. |
|  | RCL | | Art. 9 | 13) w przypadku art. 9:  a) wskazania wymaga, w który punkt zakresu spraw regulowanych projektowaną ustawą, zawartego w art. 1 projektu, wpisuje się regulacja dotycząca prowadzenia przez Prezesa UKE jawnego wykazu numerów telefonów. Wydaje się bowiem, że nakładanie zarówno tego jak i innych obowiązków na Prezesa UKE nie leży w zakresie spraw regulowanych projektem ustawy, co wymaga uzupełnienia,  b) wyjaśnienia wymaga, w jaki sposób Prezes UKE prowadzi jawny wykaz numerów telefonów – uzasadnienie w tym zakresie wskazuje, że jest on prowadzony w systemie teleinformatycznym Prezesa UKE – powyższe nie znajduje jednak odzwierciedlenia w projekcie, co wymaga uzupełnienia.  Wyjaśnienia także wymaga, czy wykaz ten jest rejestrem publicznym. Ponadto regulacja powinna wskazywać jakie dane są gromadzone  w wykazie, a także określać cel prowadzenia wykazu,  c) wyjaśnienia wymaga ograniczenie podmiotów, które mogą zgłosić wniosek o wpis do wykazu numerów telefonów do jednostek sektora finansów publicznych, o których mowa w art. 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, banków oraz  przedsiębiorców telekomunikacyjnych, przy jednoczesnym pominięciu innych podmiotów  posiadających numery służące wyłącznie do odbierania połączeń głosowych np. spółdzielczych kas oszczędnościowo-kredytowych,  d) doprecyzować należy dane, które należy podać we wniosku o wpis do wykazu, dotyczące wnioskodawcy – obecnie projektowany przepis art. 9 ust. 4 określa, że wniosek zawiera jedynie „wskazanie podmiotu”, co wydaje się być określeniem zbyt ogólnym,  e) w przypadku projektowanego ust. 6 proponuje się doprecyzować, że Prezes UKE dokonuje wpisu w terminie 5 dni od dnia otrzymania poprawnie wypełnionego/kompletnego  wniosku o wpis,  f) w przypadku ust. 9 doprecyzowania wymaga, że wycofanie dotyczy wycofania wpisu numeru z wykazu (wniosek o wycofanie numeru z wykazu), a nie wycofania wniosku, o którym mowa w ust. 2 i 3. Ponadto doregulować należy w projekcie elementy tego wniosku, podobnie jak w przypadku wniosku o wpis do wykazu; | **Uwaga uwzględniona w zakresie uzupełnienia co określa ustawa, poprzez dodanie w art. 1 pkt 1 odwołania do kompetencji Prezesa UKE (lit. a)**  **Uwaga częściowo uwzględniona (lit. b) poprzez dodanie przepisu określającego jakie dane zawiera wykaz.**  **Uwaga wyjaśniona w zakresie ograniczenia podmiotów mogących wnioskować do tzw. listy DNO (lit. c).**  Spółdzielcze kasy oszczędnościowo-kredytowe zostaną dodane jako podmioty uprawnione. Jednocześnie w ocenie projektodawcy, po pierwsze, właściwe do uzupełnienia katalogu podmiotów uprawnionych jest etap konsultacji publicznych, opiniowania oraz uzgodnień. Po drugie, znaczne poszerzenie katalogu powinno być poprzedzone oceną ex post wprowadzonych rozwiązań związanych z funkcjonowaniem listy. Nie jest możliwe szczegółowe oszacowanie zainteresowanie wpisem na wykaz numerów telefonów służących wyłącznie do odbierania połączeń głosowych, a więc liczbą wpisów do wykazu. |
|  | MKSS | | Art. 9 ust. 12 | Odnosząc się do kwestii blokowania połączeń zasadne jest rozszerzenie zakresu projektowanego art. 9 ust. 12 o możliwość blokowania także połączeń telefonicznych wykorzystujących jako identyfikację numer z wykazu numerów telefonów służących wyłącznie do odbierania połączeń głosowych (nie tylko połączeń inicjowanych). | **Uwaga wyjaśniona**  Takie połączenia będą blokowane na podstawie ogólnych przepisów o przeciwdziałaniu spoofingowi. |
|  | RCL | | Art. 10 | 14) zgodnie z art. 10 ust. 1 projektu operatorzy mogą zawrzeć z Prezesem UKE porozumienie określające środki organizacyjne i techniczne, które będą stosowali przy realizacji obowiązków, o których mowa w art. 8. Zauważenia jednak wymaga, że obowiązek,  o którym mowa w art. 8 dotyczy przedsiębiorców telekomunikacyjnych, w tym zakresie wskazany przepis wymaga więc korekty. Odnosząc się jednocześnie do kwestii samych porozumień:  a) projektowaną regulację należy uzupełnić o niezbędne minimalne elementy porozumienia, które miałyby zastosowanie do wszystkich operatorów/przedsiębiorców telekomunikacyjnych zawierających porozumienie,  b) wyjaśnienia wymaga, jakie jeszcze, oprócz blokowania numeru i ukrywania identyfikacji numeru, usługi telekomunikacyjne będące skutkiem wprowadzonych środków  technicznych i organizacyjnych, o których mowa w art. 10 ust. 1 (wskazany przepis odsyła w tym zakresie do art. 8 projektu) będzie świadczyć operator, za których niewykonanie bądź nienależyte wykonanie, w przypadku poprawnego wykonywania porozumienia, nie poniesie on odpowiedzialności; | **Uwaga nieuwzględniona co do doregulowania porozumienia antyspoofing’owego**  z projektowanych przepisów wynikają m.in.: strony porozumienia, jego przedmiot wraz z celem jego zawarcia, kontrola porozumienia oraz szczególne skutki jest zawarcia i stosowania. Reasumując, minimalne elementy porozumienia są już określone w projekcie. Z kolei środki organizacyjne i techniczne jakie będą stosowali przedsiębiorcy są kwestią zbyt szczegółową by była uregulowana na poziomie ustawowym. Z tego powodu te kwestie będą ujęte w samym porozumieniu.  **Uwaga wyjaśniona w zakresie mogących mieć zastosowanie środków technicznych i organizacyjnych**  W ocenie projektodawcy, tak jak wskazał RCL, tymi środkami sąblokowanie połączenia głosowego albo ukrycie identyfikacji numeru wywołującego dla użytkownika końcowego. Należy jednak podkreślić, że stroną porozumienia, w przypadku jego zawarcia, będzie Prezes UKE, który jest wyspecjalizowanym organem regulacyjnym w dziedzinie rynku usług telekomunikacyjnego i nie jest zasadne ograniczanie wprost katalogu środków na gruncie projektowanej ustawy. |
|  | MS | | Art. 11 ust. 1 | Za celowe uznać należy wprowadzenie w **art. 11 ust. 1** projektu podstawy prowadzenia listy ostrzeżeń obejmującej domeny internetowe, które służą do wyłudzeń danych i środków finansowych użytkowników Internetu. Jednak spójność tej koncepcji zaburza objęcie listą ostrzeżeń domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub identyfikatora użytkownika wywołującego połączenie głosowe oraz uniemożliwienia dostępu do tych stron. | **Uwaga wyjaśniona**  Wskazać należy, że przepis przewiduje możliwość, a nie obowiązek, zawarcia porozumienia, którego przedmiotem będzie prowadzenie i utrzymywanie jawnej listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i środków finansowych użytkowników internetu oraz uniemożliwianie dostępu do tych stron. W przypadku zawarcia porozumienia, zgodnie z art. 11 ust. 3, lista ostrzeżeń będzie prowadzona i udostępniana przez CSIRT NASK. |
|  | RCL | | Art. 11 | w przypadku projektowanego art. 11 należy podkreślić, że przewidywane jako zawartość projektowanego porozumienia zasady zgłaszania domen, wpisywania i oraz usuwania tych domen z listy ostrzeżeń (o których mowa w ust. 5) stanowią materię rangi ustawowej i powinny zostać określone przepisami ustawy, podobnie jak Projektodawca to uczynił w przypadku art. 4-6 dla nadużycia, o którym mowa w art. 3 ust. 1 pkt 2. Powyższe dotyczy także prowadzenia jawnej listy, o której mowa w art. 11 ust. 1 projektu oraz zadań i kompetencji poszczególnych organów odpowiedzialnych za zwalczanie nadużyć, a wskazanych obecnie jako strony porozumienia w art. 11 ust. 4. Ewentualne doprecyzowania przepisów ustawowych powinny zostać uregulowane w przepisach wykonawczych do ustawy. Takie rozwiązanie pozwoli na rezygnację z regulowania tej materii w drodze porozumienia i rezygnację z regulacji dostosowujących zawartych w art. 22 projektu. Ponadto wskazać należy, że projektowana regulacja nie określa procedury odwoławczej od decyzji o wpisaniu na listę ostrzeżeń, co wymaga uzupełnienia. | **Uwaga nieuwzględniona**  Minimalne elementy porozumienia są już określone w projektowanych przepisach rangi ustawowej.  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 jako środek o charakterze samoregulacji funkcjonuje bardzo dobrze, z korzyścią dla użytkowników. Praktyka potwierdza to, że to rozwiązanie jest właściwe w stosunku do „oszukańczych” domen. Lista ostrzeżeń jest jawna i spełnia wymogi transparentności. Jednocześnie funkcjonowanie listy wiąże się z uprawnieniem (a nie obowiązkiem) zablokowania dostępu do stron www. wpisanych na listę. |
|  | RCL | | Art. 11 | a) ust. 1:  - wyjaśnienia wymaga, czy nadużycie w komunikacji elektronicznej wskazane w tym przepisie wpisuje się w katalog nadużyć określony w art. 3 ust. 1 projektu, czy jest to kolejne nadużycie niewymienione w tym otwartym katalogu – co wymagałoby uzupełnienia,  - regulację dotyczącą projektowanego porozumienia należy uzupełnić o katalog niezbędnych elementów tego porozumienia,  b) ust. 2 – wyjaśnienia wymaga, co oznacza, że jawna lista ostrzeżeń dotyczących domen internetowych, które służą do nieuprawnionego wykorzystania numeru lub  identyfikatora użytkownika wywołującego połączenie głosowe jest elementem porozumienia,  c) ust. 3 – zgodnie z tym przepisem CSIRT NASK opracowuje, prowadzi i utrzymuje jawną listę ostrzeżeń, natomiast jak wskazano w ust. 1 - porozumienie dotyczy prowadzenia  i utrzymywania jawnej listy ostrzeżeń – kwestia różnicy w zakresie zadań podmiotu prowadzącego listę wymaga wyjaśnienia albo ujednolicenia. Dodatkowo uregulować należy  sposób prowadzenia tej listy i zakres danych/informacji w niej zawartych,  d) ust. 6 – mając na uwadze, że porozumienia, o których mowa w ust. 1 i 2, zawierane są także w zakresie uniemożliwienia dostępu do stron służących do wyłudzeń, wyjaśnienia  wymaga określona w ust. 6 jedynie możliwość, a nie obowiązek, uniemożliwiania, przez przedsiębiorcę telekomunikacyjnego, użytkownikom internetu dostępu do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę, o której mowa w ust. 1; | Uwaga **wyjaśniona**   1. Złośliwe domeny internetowe wykorzystywane są często jako część ataków smishingowych. Jest to więc narzędzie wykorzystywane przy dokonywaniu ww. nadużyć. 2. W porozumieniu będą określone pewne kwestie związane z funkcjonowaniem listy ostrzeżeń w szczególności uniemożliwianie dostępu do tych domen. 3. Pewne aspekty funkcjonowania listy zastrzeżeń będą określone w porozumieniu. Samo opracowanie listy będzie zadaniem CSIRT NASK. 4. W porozumieniu będą określone szczegóły techniczne i organizacyjne związane z procesem uniemożliwiania dostępu. |
|  | RCL | | Art. 12 | odnosząc się do projektowanego art. 12 ust. 1 – wyjaśnienia wymaga pojęcie „aktywnego konta pocztowego” jako niewystępującego w systemie prawa. Ponadto zwrócić należy uwagę na specjalistyczne określenia wskazane w części wspólnej tego przepisu – potwierdzenia w tym wypadku wymaga potrzeba umieszczenia w akcie rangi ustawowej przepisów technicznych, które mogą ulegać częstym modyfikacjom. Dodatkowo, jak się wydaje, doprecyzowania wymaga obowiązek stosowania tych mechanizmów – brak bowiem wskazania przedmiotu tego obowiązku, co powoduje konieczność uzupełnienia przepisu bądź wyjaśnienia braku tego uzupełnienia w uzasadnieniu do projektu; | **Uwaga uwzględniona poprzez usunięcie odniesienia „do aktywnego konta pocztowego”** |
|  | MRiT | | Art. 12 ust. 2 | w odpowiedzi na pismo z 15 czerwca br. (znak sprawy: DRC.WL.06110.5.2022) Ministerstwo Rozwoju i Technologii proponuje dodać do art. 12 ustępu 2 o brzmieniu:  *"2. 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)."*  W ostatnich miesiącach nasiliły się 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. Innym zagrożeniem dla użytkowników są fałszywe krótkie wiadomości tekstowe SMS. Oszuści podszywając się pod zaufane instytucje próbują nakłonić nieświadome ofiary do ujawnienia danych osobowych, informacji o karcie kredytowej czy zainfekować urządzenie poprzez kliknięcie w link w wiadomości. Zjawisko to występuje pod nazwą smishingu. W tej sytuacji konieczne jest wprowadzenia odpowiednich przepisów dotyczących zwalczania nadużyć w komunikacji elektronicznej. Proponowane rozwiązania mają służyć stworzeniu odpowiednich ram prawnych do podejmowania działań w zakresie zapobiegania nadużyciom w komunikacji elektronicznej przez przedsiębiorców telekomunikacyjnych, a w dalszej perspektywie pozwolą w większym stopniu niż obecnie ograniczyć skalę nadużyć i chronić bezpieczeństwo użytkowników. Kwestia zwalczania nadużyć nie jest regulowana w Europejskim Kodeksie Łączności Elektronicznej oraz nie była dotychczas regulowana w ustawie - Prawo telekomunikacyjne. | **Uwaga uwzględniona** |
|  | MKSS | | Art. 12 ust. 2 | W art. 12 ust. 2 projektu na podmioty publiczne został nałożony obowiązek wykorzystywania mechanizmów zapewnienia bezpieczeństwa korzystania z poczty elektronicznej. Obowiązek ten powinien dotyczyć również wewnętrznej infrastruktury teleinformatycznej podmiotu publicznego, co przyczyniłoby się do zwiększenia bezpieczeństwa zasobów wewnętrznych wykorzystywanych anych przez te podmioty. | **Uwaga wyjaśniona**  Obowiązki w zakresie bezpieczeństwa systemów informatycznych są już nałożone na podmioty publiczne w rozporządzeniu Rady Ministrów w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych. |
|  | MKSS | | Art.12 | Projektowany art. 12 ust. 3, zgodnie z którym Prezes Urzędu Komunikacji Elektronicznej uzyska możliwość przeprowadzania kontroli podmiotów publicznych - w tym służb specjalnych, w zakresie realizacji obowiązku korzystania z poczty elektronicznej wykorzystującej określone mechanizmy bezpieczeństwa, wymaga dodatkowej analizy. Należy zauważyć, że w projektowanych regulacjach nie zostały określone zasady przeprowadzania takiej kontroli, w szczególności w odniesieniu do używanych zabezpieczeń o charakterze niejawnym. W projektowanym art. 12 ust. 4, w zakresie szczegółowych regulacji dotyczących kontroli przeprowadzanej przez Prezesa UKE, projektodawca odsyła natomiast do przepisów ustawy z dnia 16 lipca 2004 r. - *Prawo telekomunikacyjne* (Dz. U. z 2021 r. poz. 576, z późn. zm.). Należy jednak wskazać, że jednostki organizacyjne służb specjalnych zostały wyłączone spod działania przepisów dotyczących kontroli wynikających z ustawy *Prawo telekomunikacyjne* na podstawie art. 205 ust. 1 tej ustawy.  Wobec powyższego zachodzi uzasadniona wątpliwość, czy przepisy projektowanej ustawy będą miały zastosowanie do służb specjalnych. Aby rozwiać te wątpliwości proponuję dodanie w projektowanej ustawie przepisu wyłączającego możliwość przeprowadzania przez Prezesa Urzędu Komunikacji Elektronicznej kontroli wykorzystania przez służby specjalne mechanizmów bezpieczeństwa poczty elektronicznej. | **Uwaga wyjaśniona**  W zakresie kontroli z niniejszej ustawy będzie obowiązywało wskazane wyłączenie z art. 205 ust. 1 ustawy - Prawo telekomunikacyjne. W związku z powyższym nie jest konieczne ponowne uregulowanie tej kwestii w samej ustawie. |
|  | MON | | Art. 12 | 1. W **art. 12** proponuje się dodać ust. 5 i 6 w brzmieniu:   *„5. Dostawca poczty elektronicznej, o którym mowa w ust. 1, ma obowiązek przechowywania, przez okres nie krótszy niż 90 dni, rejestrów logowań do obsługiwanych przez siebie skrzynek poczty elektronicznej, zawierających co najmniej datę, godzinę uszczegółowioną do 1 sekundy, adres IP oraz port przypisany użytkownikowi w trakcie połączenia przez przedsiębiorcę telekomunikacyjnego.*  *6. Dostawca poczty elektronicznej nieodpłatnie udostępnia dane, o których mowa w ust. 5, organom państwa uprawnionym na podstawie odrębnych przepisów, na potrzeby prowadzonych przez nie postępowań.”.*  4. Jednocześnie, w konsekwencji przyjęcia proponowanych zmian, zasadnym wydaje się rozważenie wprowadzenia regulacji mających na celu wzmocnienie skuteczności pozyskiwania danych, o których mowa w art. 12 ust. 5, przez organ państwowy, np. przez wprowadzenie kontroli Prezesa UKE na zasadach analogicznych jak w art. 12 ust. 3 projektu.  W związku z dynamicznym rozwojem nowych technologii oraz coraz bardziej kreatywnymi sposobami wykorzystywania ich przez osoby popełniające czyny zabronione, organy ścigania muszą niejednokrotnie sięgać po dane związane z użytkowaniem poczty elektronicznej.  Z uwagi na brak obecnie przepisów nakładających na dostawców poczty elektronicznej obowiązek gromadzenia danych na temat adresów IP wraz z portami przypisanymi przez właściwego przedsiębiorcę telekomunikacyjnego w czasie logowań, znacznie utrudnione jest ściganie sprawców przestępstw wykorzystujących pocztę elektroniczną do popełniania czynów zabronionych. Wynika to z faktu wykorzystania przez większość przedsiębiorców telekomunikacyjnych technologii CGNAT i NAT w przypadku przydzielania abonentom adresów IPv4. W praktyce oznacza to przypisanie jednego adresu publicznego bardzo dużej liczbie abonentów w tym samym czasie, co bardzo utrudnia, a często uniemożliwia ustalenie urządzenia końcowego, które korzystało z danego adresu IP. Z uwagi na brak możliwości nakazania przedsiębiorcom telekomunikacyjnym wykorzystywania jedynie adresów IPv6, które rozwiązują ten problem – proponowane zmiany są zasadne. Wprowadzenie wyżej wymienionych przepisów nie spowoduje powstania po stronie dostawców poczty elektronicznej znacznych kosztów, jest również w pełni wykonalne z technicznego punktu widzenia, a przechowywanie wymienionych w proponowanym ust. 5 danych jest niezbędne do sprawnego ścigania sprawców przestępstw. | **Uwaga nieuwzględniona**  Należy wskazać, że celem przepisu jest uregulowanie obowiązków z zakresu bezpieczeństwa poczty elektronicznej, stosowania mechanizmów uwierzytelnienia poczty elektronicznej. Nie jest celem ustawy wprowadzanie obowiązków retencyjnych, które wykraczają poza kwestie walki z nadużyciami w komunikacji elektronicznej. Mają szersze, systemowe skutki dla różnego rodzaju postępowań prowadzonych przez służby.    Dostawcy usług poczty elektronicznej kwalifikują się do kategorii dostawców usług komunikacji interpersonalnej niewykorzystujących numerów („NICS”) (które zostaną uregulowane w PKE) a także usług świadczonych drogą elektroniczną. Należy wskazać, że ta kategoria podmiotów nie jest również w PKE objęta przepisami retencyjnymi. Dyrektywa ustanawiająca Europejski Kodeks Łączności Elektronicznej wyłącza tę kategorię podmiotów (dostawców NICS) z obowiązków związanych z ogólnym zezwoleniem, tj. nie podlegają wpisowi do rejestru przedsiębiorców telekomunikacyjnych. Brak jest zatem oficjalnych danych tych podmiotów. Egzekwowanie stosowania przepisów mogłoby być znacząco utrudnione, gdyż często przedsiębiorcy Ci mają siedziby za granicą. W efekcie zatem wprowadzone obowiązki obciążyły by de facto polskich dostawców takich usług, stawiając ich mniej korzystnej sytuacji niż konkurenci z zagranicy. Naraziłoby to również te podmioty na dodatkowe koszty retencjonowania danych, które nie są im potrzebne. Większy zakres przechowywanych danych wymagałby posiadania pojemniejszych, bezpiecznych serwerów, zakupu bezpiecznego oprogramowania itp.    Podkreślenia wymaga również fakt, że generalny obowiązek retencji danych telekomunikacyjnych został zakwestionowany przez TSUE. Trybunał w licznych wyrokach odnosił się w restrykcyjny sposób do kwestii gromadzenia danych pochodzących z komunikacji elektronicznej i ich udostępniania uprawnionym podmiotom.  Wprowadzanie nowych obowiązków retencyjnych, w odniesieniu do kolejnych grup podmiotów może spotkać się z zarzutem niezgodności z orzecznictwem TSUE.  W ramach UE ciągle trwają prace grupy roboczej ds. współpracy w sprawach karnych COPEN dotyczących wspólnego podejścia do retencji danych w świetle dyrektywy 2002/58/UE o prywatności oraz orzecznictwa TSUE. Grupa rozważa m.in. objęcie obowiązkiem retencyjnym dostawców NICS, poddania retencji adresów IP. Wprowadzanie nowych obowiązków retencyjnych w oderwaniu od prac tej grupy, zapadłych wyroków TSUE jest przedwczesne.    Ponadto, ustawa o świadczeniu usług drogą elektroniczną oraz ustawy kompetencyjne służb zawierają już pewne regulacje dotyczące udostępniania służbom danych zbieranych przez dostawców usług (np. art. 18 uśude). |
|  | RCL | | Art. 13 | w przypadku obowiązku rejestracji danych o usługach telekomunikacyjnych, o którym mowa w art. 13 ust. 1, projektowaną regulację należy uzupełnić o wskazanie danych podlegających rejestracji, a także miejsca i sposobu prowadzenia tej „rejestracji” (czy to będzie rejestr danych o usługach prowadzony w systemie teleinformatycznym?). Ponadto, korekty wymaga przepis ust. 2 w zakresie okresu przechowywania tych danych – wskazanie okresu co najmniej 12 miesięcy oznacza nieokreślony okres przechowywania – termin ten powinien więc zostać doprecyzowany; | **Uwaga częściowo uwzględniona**  **w zakresie okresu przechowywania danych**  Przepis koresponduje z regulacją zawartą w art. 168 ustawy - Prawo telekomunikacyjne i był na niej wzorowany. Zgodnie z tym przepisem dostawca publicznie dostępnych usług telekomunikacyjnych jest obowiązany do rejestracji danych o wykonanych usługach telekomunikacyjnych, w zakresie umożliwiającym ustalenie należności za wykonanie tych usług oraz rozpatrzenie reklamacji.  Dane te dostawca przechowuje co najmniej przez okres 12 miesięcy, a w przypadku wniesienia reklamacji - przez okres niezbędny do rozstrzygnięcia sporu.    Rodzaj zbieranych danych wynika z definicji tajemnicy telekomunikacyjnej zawartej w art. 159 ustawy Prawo telekomunikacyjne i nie jest konieczne ich wskazywanie. Również w przypadku art. 168 Pt uznano, iż przepis powinien być przyszłościowy, a zatem katalog przetwarzanych danych będzie zależny od rodzaju usługi i stosowanej technologii.    W zakresie miejsca i sposobu prowadzenia „rejestracji” zasadne jest pozostawienie tej kwestii, podobnie jak w ustawie Pt, do decyzji przedsiębiorcy.    Proponuje się zmianę wyrażenia „co najmniej przez okres 12 miesięcy” na „przez okres 12 miesięcy”. |
|  | MSUE | | Art. 14 ust. 2 | 1. Zgodnie z projektowanym art. 14 ust. 2 ustawy przedsiębiorcy telekomunikacyjni mogą przetwarzać i wzajemnie udostępniać również komunikat elektroniczny w celu identyfikacji, zapobiegania i zwalczania smishingu. Ponadto, zgodnie z ust. 3 tego przepisu, przedsiębiorca telekomunikacyjny może przetwarzać:   1) treści krótkich wiadomości tekstowych (SMS), oraz  2) dane o usługach telekomunikacyjnych, które nie zostały przez tego przedsiębiorcę wykonane w związku z realizacją obowiązku, o którym mowa w art. 4 ust. 6 lub uprawnienia, o którym mowa w art. 7  – w celu realizacji obowiązku, o którym mowa w art. 3 ust. 2, art. 4 ust. 6 i art. 8 oraz realizacji uprawnienia, o którym mowa w art. 7, a także na cele związane z dochodzeniem roszczeń.  Wydaje się, że przywołane przepisy umożliwiają ingerencję w treść komunikatów elektronicznych oraz krótkich wiadomości tekstowych. Tymczasem na mocy art. 5 ust. 1 *dyrektywy 2002/58/WE Parlamentu Europejskiego i Rady z dnia 12 lipca 2002 r. dotyczącej przetwarzania danych osobowych i ochrony prywatności w sektorze łączności elektronicznej (dyrektywa o prywatności i łączności elektronicznej)* państwa członkowskie mają zapewnić, poprzez ustawodawstwo krajowe, poufność komunikacji i związanych z nią danych o ruchu. W szczególności zakazane powinno być słuchanie, nagrywanie, przechowywanie lub inne rodzaje przejęcia lub nadzoru komunikatu i związanych z nim danych o ruchu przez osoby inne niż użytkownicy, bez zgody zainteresowanych użytkowników, z wyjątkiem upoważnienia zgodnego z art. 15 ust. 1.  Z kolei zgodnie z art. 15 ust. 1 dyrektywy 2002/58/WE państwa członkowskie mogą uchwalić środki ustawodawcze w celu ograniczenia zakresu praw i obowiązków przewidzianych w art. 5, 6, art. 8 ust. 1–4, i art. 9 tej dyrektywy, gdy takie ograniczenia stanowią 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 elektronicznej.  Możliwe jest zatem ustanowienie środków w tym zakresie, po pierwsze na podstawie zgody zainteresowanego użytkownika, a po drugie, w celu zapobiegania niedozwolonemu używaniu systemów łączności elektronicznej - pod warunkiem jednak, że środki te będą niezbędne, właściwe i proporcjonalne do tego celu.  W tym zakresie wyjaśnienia przez projektodawcę wymaga sposób przetwarzania informacji, o których jest mowa w projektowanym art. 14 ust. 2 i ust. 3 ustawy i tego, czy treści komunikatów elektronicznych oraz treści krótkich wiadomości tekstowych będą pozyskiwane od samych zainteresowanych użytkowników (np. tak jak to sugeruje obecne brzmienie art. 4 ust. 1 projektu, zgodnie z którym CSIRT NASK na podstawie otrzymanych od odbiorców krótkich wiadomości tekstowych (SMS) monitoruje występowanie smishingu), czy też przetwarzanie to będzie odbywało się w inny sposób, np. automatyczny, i będzie polegało na filtrowaniu treści komunikatów pod kątem występowania w nich niedozwolonych treści.  Uzasadnienie projektu ustawy nie zawiera w tym zakresie wyjaśnień, a kwestia ta jest istotna do właściwej oceny zgodności projektowanych rozwiązań z przepisami dyrektywy 2002/58/WE, jak również - jak się zdaje - z *rozporządzeniem 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)*. Należy bowiem pamiętać, że jakakolwiek ingerencja w treść komunikatów łączności elektronicznej powinna być dozwolona jedynie w bardzo jasno określonych warunkach i w konkretnych celach oraz powinna podlegać odpowiednim zabezpieczeniom przed nadużyciami. | **Uwaga uwzględniona**  Proponuje się rozszerzenie uzasadnienia projektowanej ustawy o wskazane w uwadze zagadnienia.  Przy okazji należy wskazać, iż projektowane przepisy nie przewidują ingerencji w treść komunikatu elektronicznego. Tajemnica telekomunikacyjna podlega wyłączeniu na podstawie art. 159 ust. 2 pkt 4 PT, wobec której przepisy projektowanej ustawy stanowią *lex specialis*.  W ramach wykonywania obowiązku na rzecz bezpieczeństwa publicznego oraz zapobiegania, dochodzenia, wykrywania i karania przestępstw kryminalnych lub niedozwolonego używania systemów łączności elektronicznej przedsiębiorcy telekomunikacyjni uprawnieni będą do blokowania wiadomości (SMS) po porównaniu jej ze wzorcem określonym przez NASK lub po automatycznej identyfikacji wykonywanej w oparciu o system informatyczny przedsiębiorcy. Nie podlega ingerencji treść wiadomości – zostaje ona zablokowana.  Należyte wyjaśnienia zostaną zawarte w uzasadnieniu ustawy. |
|  | MS | | Art. 14 ust. 4 | Należy również wskazać, że w projektowanym **art. 14 ust. 4** zostało przewidziane wprowadzenie ograniczenia dla praw osób, których dane dotyczą, wynikających z przepisów 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.), dalej „RODO”. Tego rodzaju ograniczenia, zgodnie z art. 23 RODO, mogą być wprowadzone aktem prawnym prawa państwa członkowskiego, który zawierać będzie zapisy wskazane w art. 23 ust. 2 RODO. Opiniowany projekt nie realizuje w pełni wymogów tego przepisu. | **Uwaga uwzględniona**  Proponuje się rozszerzenie uzasadnienia o wskazane w uwadze zagadnienia, odnosząc się do relewantnych zapisów wskazanych w art. 23 ust. 2 RODO. |
|  | MSUE | | Art. 14 ust. 4 | 1. Na podstawie art. 14 ust. 4 projektu ustawy do przetwarzania danych osobowych przez przedsiębiorców telekomunikacyjnych nie stosuje się przepisu art. 14 i 15 rozporządzenia 2016/679 w zakresie, w jakim jest to niezbędne dla identyfikacji, zapobiegania oraz zwalczania przestępstw na szkodę przedsiębiorcy telekomunikacyjnego.   Zwracam zatem uwagę na to, że na podstawie art. 23 ust. 1 rozporządzenia 2016/679 prawo Unii lub prawo państwa członkowskiego, któremu podlegają administrator danych lub podmiot przetwarzający, może aktem prawnym ograniczyć zakres obowiązków i praw przewidzianych w art. 12–22 i w art. 34, a także w art. 5 – o ile jego przepisy odpowiadają prawom i obowiązkom przewidzianym w art. 12–22 – jeżeli ograniczenie takie nie narusza istoty podstawowych praw i wolności oraz jest w demokratycznym społeczeństwie środkiem niezbędnym i proporcjonalnym, służącym określonym w tym ustępie celom. Można zatem wprowadzić ograniczenie w powyższym zakresie, które ma służyć np. celowi zapobiegania przestępczości, prowadzenia postępowań przygotowawczych, wykrywania lub ścigania czynów zabronionych lub wykonywania kar, w tym ochronie przed zagrożeniami dla bezpieczeństwa publicznego i zapobieganiu takim zagrożeniom (lit. d)), czy innym ważnym celom leżącym w ogólnym interesie publicznym Unii lub państwa członkowskiego, w szczególności ważnemu interesowi gospodarczemu lub finansowemu Unii lub państwa członkowskiego, w tym kwestiom pieniężnym, budżetowym i podatkowym, zdrowiu publicznemu i zabezpieczeniu społecznemu (lit. e)). Jednak przy wprowadzaniu takich regulacji zasadne jest przedstawienie uzasadnienia wykazującego, że projektowane środki są niezbędne i proporcjonalne do takich celów, zgodnie z treścią wspomnianego art. 23 ust. 1 rozporządzenia 2016/679. Uzasadnienie projektu nie odnosi się do tej kwestii, potrzebne jest zatem jego uzupełnienie pod tym kątem.  Ponadto na podstawie art. 23 ust. 2 rozporządzenia 2016/679 akt prawny, który ma wprowadzać takie ograniczenia, musi zawierać szczegółowe przepisy przynajmniej – w stosownym przypadku – o:   1. celach przetwarzania lub kategorii przetwarzania; 2. kategoriach danych osobowych; 3. zakresie wprowadzonych ograniczeń; 4. zabezpieczeniach zapobiegających nadużyciom lub niezgodnemu z prawem dostępowi lub przekazywaniu; 5. określeniu administratora lub kategorii administratorów; 6. okresach przechowywania oraz mających zastosowanie zabezpieczeniach z uwzględnieniem charakteru, zakresu i celów przetwarzania lub kategorii przetwarzania; 7. ryzykach naruszenia praw lub wolności osoby, której dane dotyczą; oraz 8. prawie osób, których dane dotyczą, do uzyskania informacji o ograniczeniach, o ile nie narusza to celu ograniczenia.   Niezbędne jest więc wykazanie przez projektodawcę, że wymogi te zostaną spełnione oraz wskazanie, w jaki sposób. Uzasadnienie projektu ustawy nie zawiera wyjaśnień w tym zakresie. | **Uwaga uwzględniona**  Proponuje się rozbudowanie uzasadnienia o poruszone kwestie dotyczące spełnienia warunków z art. 23 ust. 1 i 2 RODO. |
|  | MS | | Art. 15 | Wadliwa techniczne jest konstrukcja przepisów o karach pieniężnych **projektowanych w art. 15**. Przepisy te nie spełniają elementarnych wymagań § 81a *Zasad techniki prawodawczej.* W przepisach o karach pieniężnych należy: dokładnie określić hipotezę normy sankcjonowanej (wskazać kto i w jakich okolicznościach może zostać ukarany daną karą pieniężną), określić czyn zabroniony, określić podmiot uprawniony do nałożenia kary oraz procedurę jej nakładania, jak również określić sankcję. Projektowane rozwiązania nie uwzględniają też tego, że podstawowym aktem prawnym zawierającym regulację w zakresie administracyjnych kar pieniężnych jest ustawa z dnia 14 czerwca 1960 r. – *Kodeks postępowania administracyjnego* (Dz. U. z 2021 r. poz. 735, z późn. zm.). | **Uwaga uwzględniona poprzez doprecyzowanie przepisów o karach pieniężnych** |
|  | MS | | Art. 15 ust. 5 | W zakresie regulacji dotyczących kar pieniężnych zwrócić należy również uwagę na projektowany **art. 15 ust. 5**, zgodnie z którym Prezes UKE będzie mógł nakładać administracyjne kary pieniężne na kierownika podmiotu publicznego. Podmiotem publicznym, zgodnie z definicją zawartą w art. 2 pkt 6 projektu ustawy, jest podmiot, o którym mowa w art. 4 pkt 7-15 ustawy z dnia 5 lipca 2018 r. *o krajowym systemie cyberbezpieczeństwa* (Dz. U. z 2020 r. poz. 1369, z późn. zm.). Wskazania wymaga, że k.p.a. normuje m.in. postępowanie przed organami administracji publicznej w należących do właściwości tych organów sprawach indywidualnych rozstrzyganych w drodze decyzji administracyjnych albo załatwianych milcząco oraz nakładanie lub wymierzanie administracyjnych kar pieniężnych lub udzielanie ulg w ich wykonaniu (art. 1 pkt 1 i 5 k.p.a.). Pomiotami mogącymi być stroną postępowania administracyjnego – stosownie do art. 29 k.p.a. – są osoby fizyczne i osoby prawne, a gdy chodzi o państwowe i samorządowe jednostki organizacyjne i organizacje społeczne – również jednostki nieposiadające osobowości prawnej. Zgodnie natomiast z art. 189b k.p.a. *przez administracyjną karę pieniężną rozumie się określoną w ustawie sankcję o charakterze pieniężnym, nakładaną przez organ administracji publicznej, w drodze decyzji, w następstwie naruszenia prawa polegającego na niedopełnieniu obowiązku albo naruszeniu zakazu ciążącego na osobie fizycznej, osobie prawnej albo jednostce organizacyjnej nieposiadającej osobowości prawnej.* Biorąc pod uwagę szeroki katalog podmiotów wchodzących w skład definicji podmiotu publicznego, powinno dokonać się weryfikacji, czy na kierownika każdego podmiotu publicznego będzie mogła zostać nałożona kara pieniężna. Zauważyć bowiem należy, że zgodnie z definicją z art. 2 pkt 6 projektu ustawy podmiotami publicznymi będą m.in. organy władzy publicznej, w tym organy administracji rządowej, organy kontroli państwowej i ochrony prawa oraz sądy i trybunały (art. 9 pkt 1 ustawy *o finansach publicznych*). Nie jest natomiast możliwe nałożenie kary pieniężnej na którykolwiek z wymienionych organów, ponieważ podmiotami obowiązku prawnego, w następstwie niedopełnienia którego nakładana jest administracyjna kara pieniężna, mogą być osoby fizyczne, osoby prawne i jednostki organizacyjne nieposiadające osobowości prawnej (por. podmioty będące stroną postępowania administracyjnego – art. 29 k.p.a.).. Natomiast przepisy k.p.a. nie regulują postępowań w sprawach wynikających z nadrzędności i podległości organizacyjnej w stosunkach między organami państwowymi i innymi państwowymi jednostkami organizacyjnymi. | **Uwaga wyjaśniona**  Zamiarem projektodawcy jest możliwość nałożenia kary na kierownika podmiotu –piastuna funkcji za niedopełnienie obowiązku. Można sobie wyobrazić sytuację, w której pomimo nałożenia kary na podmiot publiczny, obowiązek nadal nie jest wykonywany. Dlatego powinna być możliwość ukarania kierownika tego podmiotu, co powinno wywołać odpowiedni efekt prewencyjny. W przypadku organu administracji publicznej kara nie będzie nakładana na organ lecz na jego piastuna. |
|  | MS | | Art. 15 art. 16 | Niezależnie od wątpliwości dotyczących sposobu sformułowania przepisów karnych w projektowanej ustawie, które ograniczają odpowiedzialność karną tylko do fragmentu zdefiniowanych jako nadużycia w komunikacji elektronicznej działań, wątpliwości budzi również wprowadzony **dualizm karalności tych samych zachowań – na mocy art. 15 ust. 1 karą administracyjną i na podstawie art. 16 – sankcją karną,** chociażby w kontekście zasady *ne bis in idem*. | **Uwaga uwzględniona**  Ustawa przewiduje wyraźne rozgraniczenie na sankcje administracyjne (nakładane na przedsiębiorców telekomunikacyjnych lub podmioty publiczne za niezrealizowanie określonych obowiązków), a także na sankcje karne, za dopuszczenie się nadużyć w komunikacji elektronicznej. |
|  | MKSS | | Art. 15 | Należy zaproponować również uzupełnienie przepisów projektu regulujących zagadnienia czynów zabronionych oraz kar za ich popełnienie, określonych w projektowanych art. 15 ust. 1 oraz art. 16 ust. 1 przedmiotowego projektu, w szczególności w zakresie ich stosowania wobec organów państwa, których zadania są związane z ochroną bezpieczeństwa państwa. Przytoczone przepisy wprowadzają sankcje, zgodnie z którymi dokonanie nadużycia w komunikacji elektronicznej będzie zagrożone karą pieniężną (projektowany art. 15 ust. 1). Natomiast dopuszczenie się tych nadużyć w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody będzie zagrożone karą pozbawienia wolności od 3 miesięcy do lat 5. W przypadku mniejszej wagi przewidziana jest kara grzywny, ograniczenia wolności albo pozbawienia wolności do roku (projektowany art. 16 ust. 1 i 2). | **Uwaga wyjaśniona**  Przepis karny został doprecyzowany w zw. z innymi uwagami zgłoszonymi podczas konsultacji publicznych, uzgodnień i opiniowania. |
|  | RCL | | Art. 15 | 18) w przypadku przepisów o karach pieniężnych zauważyć należy:  a) w art. 15 w ust. 1 określono, że kto dokonuje nadużyć w komunikacji elektronicznej, o których mowa w art. 3 ust. 1 pkt 1, 2 lub 3, podlega karze pieniężnej. Zauważyć jednak należy, że zgodnie z art. 3 zakazane są nadużycia w komunikacji elektronicznej (wszelkie),a w szczególności te wskazane w pkt 1-3. Projektodawca określa jednak jedynie sankcje za nadużycia wskazane w pkt 1-3 pomijając fakt, że poza regulacją karną pozostają nadużycia inne – czyli, zgodnie z definicją, 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. Kwestia ta wymaga wyjaśnienia,  b) mając na uwadze zasadę określoności prawa przepis art. 15 ust. 4 zdanie drugie, zawierający odesłania do ustawy – Prawo telekomunikacyjne, należy usunąć, a projektowaną regulację uzupełnić wprost o niezbędne przepisy dotyczące m.in. wysokości kar pieniężnych oraz trybu ich egzekucji; | **Uwaga uwzględniona**  **w zakresie jakim dot. uzupełnienia przepisów karnych w innych niż poprzez odesłanie**  **Uwaga wyjaśniona w pozostałym zakresie** Jak wynika z innych uwag RCL, obowiązek podejmowania proporcjonalnych środków technicznych i organizacyjnych mających na celu zapobieganie nadużyciom w komunikacji elektronicznej i ich zwalczanie ma charakter ogólny. Jest on w pewnym zakresie doprecyzowany innymi postanowieniami projektowanej ustawy. W pozostałym zakresie, tj. w takim w jakim nie jest doprecyzowany, nie może wiązać się z ryzykiem nałożenia sankcji przez jego niestosowanie. |
|  | MS | | Art. 16 ust. 1 | projektowane w **art. 16 ust. 1** przepisy w zakresie odpowiedzialności karnej sprawców nadużyć w komunikacji elektronicznej wymagają pogłębionej analizy i korekty redakcyjnej. Z punktu widzenia ich czytelności zasadne byłoby ujęcie każdego z zachowań wyszczególnionych w punktach 1-3 w odrębnej jednostce redakcyjnej.  Zauważyć należy, że pkt 2 ww. przepisu obejmuje jedynie zachowania polegające na wysłaniu krótkich wiadomości tekstowych (SMS).  Pominięto zarówno wiadomości multimedialne MMS (przy pomocy których również dochodzi do naruszeń), wiadomości przesyłane przy pomocy komunikatorów internetowych (do wysyłania linków prowadzących do stron podszywających się pod portale społecznościowe np. Facebook – zazwyczaj dochodzi przy wykorzystaniu Messengera, zaś do wyłudzania danych kart płatniczych w atakach ukierunkowanych na sprzedających towary na platformach sprzedażowych typu OLX i Vinted – przy wykorzystaniu komunikatora WhatsApp). Zatem nadmiernie wąsko określono sposób działania sprawcy.  Pominięto również objęcie odpowiedzialnością karną działania tych sprawców, którzy w celu nakłonienia odbiorcy do określonego działania, w szczególności przekazania danych osobowych, nieświadomego rozporządzenia majątkiem, przekierowania na stronę www, żądania kontaktu telefonicznego lub instalacji oprogramowania, wysyłają wiadomości pocztą elektroniczną.  Dla zapewnienia karnoprawnej reakcji bez względu na zastosowany kanał komunikacji i ewentualny rozwój technologii, celowe jest dokonanie zmian w zakresie art. 16 pkt 2 przez zastąpienie zwrotu *krótkich wiadomości tekstowych (SMS)* określeniem *wiadomości tekstowych lub multimedialnych, w tym również przesyłanych pocztą elektroniczną* lub wskazanego w słowniczku ustawowym określenia *komunikatów elektronicznych* – zdefiniowanych jako każda informacja wymieniana lub przekazywana między określonymi użytkownikami za pośrednictwem publicznie dostępnych usług telekomunikacyjnych lub usług komunikacji interpersonalnej niewykorzystujących numerów.  Ponieważ celem działania sprawców jest zazwyczaj pozyskanie haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej – ten cel powinien zostać uwzględniony w opisie zachowań ujętych zarówno w pkt 2 i 3 w art. 16 ust. 1. | **Uwaga uwzględniona w zakresie dodania odrębnych jednostek redakcyjnych**  **Uwaga uwzględniona w zakresie rozszerzenia sposobu działania sprawcy poprzez odniesienie do wiadomości multimedialnych (MMS) lub wiadomości wysyłanych za pośrednictwem innych usług łączności interpersonalne. W związku ze zmianami będzie penalizowany nie tylko „smishing”.**  **Uwaga uwzględniona w zakresie dodania do projektowanego art. 16 ust. 1 pkt 2 i 3 odniesienia do pozyskania haseł komputerowych, kodów dostępu lub innych danych umożliwiających nieuprawniony dostęp do informacji przechowywanych w systemie informatycznym, teleinformatycznym lub sieci teleinformatycznej.** |
|  | MS | | Art. 16 | Ponadto należy postulować korektę pojęć projektowanych przepisów, polegającą na zastąpieniu wyrażenia *„rozporządzenie majątkiem”* wyrażeniem „*rozporządzenie mieniem”,* zaś wyrażenia „*przekierowanie na stronę www”* wyrażeniem „*przekierowanie na stronę internetową”*. Pojęcie *strony internetowej* posiada bowiem definicję legalną określoną w *ustawie* z dnia 4 kwietnia 2019 r. *o dostępności cyfrowej stron internetowych i aplikacji mobilnych podmiotów publicznych* (Dz. U. z 2021 r. poz. 576, z późn. zm.)1. Dodatkowo należy wskazać, że określenie przymiotnikowe *nieświadome* w odniesieniu do rozporządzenia majątkiem zawęża obszar kryminalizacji. Analizy metod działania sprawców wskazują, że pokrzywdzony jest nakłaniany do rozporządzenia mieniem w wyniku wprowadzenia go w błąd co do podmiotu, na rzecz którego dokonuje rozporządzenia. Zatem znamiona czynu określonego w art. 16 ust. 1 pkt 2 powinny obejmować zarówno świadome, jak i nieświadome rozporządzenia mieniem. Analogiczne zmiany powinny zostać wprowadzone w art. 3 projektu. Cel działania wskazany w art. 3 ust. 3 projektowanej ustawy, jakim jest doprowadzenie pokrzywdzonego do rozporządzenia mieniem powinien znaleźć odzwierciedlenie także w treści art. 16 ust. 1 pkt 3. | **Uwagi częściowo uwzględnione**  Strona www zostanie zastąpiona stroną internetową  Sformułowanie „rozporządzenie majątkiem” zostaje pozostawione bez zmian. W ocenie projektodawcy takie brzmienie przepisu zapewni szerszą ochronę przed nadużyciami w komunikacji elektronicznej. Jest to pojęcie powszechnie używane i rozumiane oraz szersze niż mienie.  Usunięty zostanie przymiotnik „nieświadome” a w uzasadnieniu zostanie dopisane, że czyn będzie obejmował świadome i nieświadome rozporządzenie mieniem. |
|  | RCL | | Art. 17 | 19) wyjaśnienia wymaga pominięcie przez Projektodawcę kwestii przedstawiania przez Prezesa UKE corocznego sprawozdania ministrowi właściwemu do spraw informatyzacji (art. 17 projektu); | **Uwaga uwzględniona**  Uzupełniono projektowany przepis o obowiązek przedstawienia sprawozdania również ministrowi właściwemu ds. informatyzacji. |
|  | MON | | Art. 17a | 1. W następstwie uwzględnienia proponowanego brzmienia art. 12 ust. 5 i 6 niezbędnym jest dodanie w projekcie po art. 17 przepisów zmieniających *ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2021 r. poz. 1214, z późn. zm.),* w brzmieniu:   *„****Art. 17a.****W ustawie z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. z 2021 r. poz. 1214 oraz z 2022 r. poz. 655) w art. 30 wprowadza się następujące zmiany:*  *1) w ust. 1 po pkt 3 dodaje się pkt 4 w brzmieniu:*  *„4) art. 12 ust. 5 ustawy z dnia … o zwalczaniu nadużyć w komunikacji elektronicznej (Dz. U. poz. …);”;*  *2) w ust. 3 po wyrazach „pkt 3” dodaje się wyrazy: „i 4”.* | **Uwaga nieuwzględniona w zw. z nieuwzględnieniem uwagi dot. art. 12 ust. 5 i 6** |
|  | RCL | | Art. 19 | 20) zgodnie z art. 19 ust. 3 - Komendant Główny Policji, Prezes UKE i przedsiębiorcy telekomunikacyjni obowiązani są do podłączenia się do systemu, o którym mowa w art. 4 ust. 3, w terminie 3 miesięcy od dnia udostępnienia przez ministra właściwego do spraw informatyzacji informacji o uruchomieniu tego systemu – zauważyć jednak należy, że przepisy projektowanej ustawy nie regulują kwestii obowiązku „podłączania się” do systemu teleinformatycznego CSIRT NASK, co wymaga uzupełnienia. | **Uwaga uwzględniona**  Zostanie dodany przepis, zgodnie z którym przedsiębiorcy telekomunikacyjni, Komendant Główny Policji, Prezes UKE obowiązani są do korzystania z systemu teleinformatycznego, mającego na celu wymianę wzorców. |
|  | MS | | OSR | Podkreślenia wymaga, że przedstawiony projekt ustawy nakłada na sądownictwo powszechne **całkowicie nowe obowiązki**. Tym samym oczywistym jest, że ich realizacja musi wiązać się ze wzmocnieniem etatowym. Nowe obowiązki powodują bowiem zwiększenie zadań i tak już znacznie obciążonego sądownictwa, a w związku z tym nie można oczekiwać, że będą one realizowane obecnymi zasobami kadrowymi bez pogorszenia sprawności postępowań.  W OSR wśród podmiotów, na które może oddziaływać projekt ustawy, nie ma SO w Warszawie – SOKiK oraz Sądu Apelacyjnego w Warszawie. Podkreślić trzeba, że takie oddziaływanie może wystąpić, biorąc pod uwagę możliwość odwołania od decyzji Prezesa UKE w przedmiocie kary pieniężnej – określonej w **art. 15** – na podstawie art. 206 ust. 2 pkt 3 *Prawa telekomunikacyjnego*. Konieczność oszacowania wpływu projektowanych rozwiązań na SOKiK, wynika także z rozwiązania przyjętego w art. 10 ust. 4 i art. 12 ust. 4. Przepisy te zawierają odesłanie do przepisów *Prawa telekomunikacyjnego* o kontroli, przy czym zastrzeżenia budzi już sama ogólnikowość takiego odesłania. *Prawo telekomunikacyjne* obejmuje szereg takich przepisów, przy czym w większości znajdują się one w rozdziale 2 *Kontrola i postępowanie kontrolne*. Przepis art. 201 *Prawa telekomunikacyjnego* przewiduje podstawę do wydania przez Prezesa URE decyzji o nałożeniu kary pieniężnej, o której mowa w art. 209, w przypadku stwierdzenia naruszeń obowiązków wynikających z przepisów prawa lub decyzji wydanej przez Prezesa UKE. Zgodnie z art. 206 ust. 2 pkt 3 *Prawa telekomunikacyjnego* decyzja taka podlega zaskarżeniu do SOKiK.  Ponadto **art. 16 ust. 1 i 2** penalizuje trzy nadużycia w komunikacji elektronicznej.  Powoduje to rozszerzenie kognicji wydziałów karnych w sądach powszechnych, zarówno w I, jak też II instancji, co nie zostało wskazane w uzasadnieniu projektu.  Podkreślenia wymaga, że wzrost liczby spraw nie może zostać precyzyjnie oszacowany, albowiem przewidziane projektem ustawy instytucje są nowe i brak jest jakichkolwiek danych umożliwiających oszacowanie tej wartości. Nadto, ani w uzasadnieniu projektu, ani w OSR nie zostały podane jakiekolwiek dane pozwalające na choćby hipotetyczne określenie liczby spraw, które trafią do sądów. Oczywistym jest, że wsparcie etatowe jest konieczne, albowiem komunikacja elektroniczna stanowi narzędzie powszechnie wykorzystywane w życiu codziennym przez współczesne społeczeństwo informacyjne i penalizowane czyny mogą występować bardzo często. Z usług dostarczanych przez przedsiębiorców telekomunikacyjnych korzysta wiele milionów osób. Usługi te są również coraz szerzej i w sposób bardziej wyszukany wykorzystywane przez przestępców w celu wyrządzenia szkód po stronie przedsiębiorców telekomunikacyjnych, użytkowników końcowych oraz osiągnięcia nienależnych korzyści.  Nowe sprawy – z art. 15 projektu ustawy – trafią do SO w Warszawie – SOKiK, a – z art. 16 projektu ustawy – do sadów rejonowych (pion karny). Zachodzi więc konieczność zapewnienia zwiększenia potencjału kadrowego tych jednostek Znając ograniczenia budżetowe wynikające z sytuacji spowodowanej pandemią COVID-19, Ministerstwo Sprawiedliwości wnosi o przydzielenie nowych etatów do: **SOKiK w liczbie: 1 etat sędziowski, 1 etat asystencki i 2 etaty urzędnicze oraz sądów rejonowych (pion karny) w liczbie: 5 etatów sędziowskich, 5 etatów asystenckich i 10 etatów urzędniczych.**  Zaznaczenia przy tym wymaga, że nie zgłasza się potrzeb na szczeblu sądów okręgowych,choć oczywistym jest, że trafią tam odwołania od orzeczeń wydanych w I instancji. **Etatypowyższe powinny zostać uruchomione od 1 stycznia 2023 r.**  Mając na względzie powyższe, modyfikacji wymaga OSR projektu w punkcie 4  *Podmioty, na które oddziałuje projekt* przez wskazanie SO w Warszawie jako podmiotu rozpoznającego odwołania od decyzji Prezesa UKE oraz sądów powszechnych (sądy okręgowe i sądy rejonowe) jako podmiotów rozpatrujących nowe sprawy karne.  W obu przypadkach nastąpi wzrost wpływu nowych spraw. Skutkiem powyższego konieczne wydaje się także uzupełnienie OSR w punkcie 6 *Wpływ na sektor finansów publicznych* i wskazanie stosownych wydatków związanych z planowanym wsparciem etatowym. | **Uwaga nieuwzględniona**  Przyjęte rozwiązania nie doprowadzą do istotnego wzrostu liczby spraw sądowych. W związku z tym, że dołączenie do porozumienia i jego realizacja będą wiązały się z domniemaniem wypełniania obowiązków wynikających z niniejszej ustawy najprawdopodobniej nie będzie wielu postępowań karnoadministracyjnych. W związku z tym nie jest konieczne wygospodarowanie nowych wydatków dla SOKIK-u. |
|  | Koordynator OSR | | Pkt 5 OSR | Ocena skutków regulacji wymaga zaprezentowania w pkt 5 OSR uzasadnienia faktu skrócenia terminu konsultacji publicznych poniżej wymaganego przepisami terminu 21 dni. | **Uwaga uwzględniona**  OSR został uzupełniony. |
|  | Koordynator OSR | | Pkt 6 OSR | Niezbędne jest również uzupełnienie pkt 6 OSR (w tym tabeli) o informacje dotyczące kosztów związanych z dodatkowymi obciążeniami nakładanymi na instytucje publiczne (UKE, NASK). Sekcja „Informacje dodatkowe” w pkt 6 OSR powinna prezentować metodykę szacunków dot. wysokości ww. kosztów, natomiast sekcja „Źródła finansowania” powinna informować  o zakładanym źródle sfinansowania tych kosztów (w tym części budżetowej, z której będą ponoszone dodatkowe wydatki oraz informacji, czy wejście w życie ustawy będzie podstawą do zwiększenia wydatków ponad dotychczasowe limity). | **Uwaga wyjaśniona**  Koszty CSIRT NASK zmieszczą się w ramach dotychczasowej dotacji podmiotowej dla CSIRT NASK. Będą również marginalne. |
|  | Koordynator OSR | | Pkt 7 OSR | Pkt 7 OSR należy uzupełnić o informacje dot. kosztów dostosowawczych dla przedsiębiorców, związanych z podleganiem nowym obowiązkom. W szczególności dotyczy to kosztów wprowadzenia przez przedsiębiorców telekomunikacyjnych rozwiązań technicznych umożliwiających blokowanie/odblokowywanie wiadomości tekstowych zawierających określone treści oraz rozwiązań umożliwiających blokowanie wybranych połączeń głosowych. | **Uwaga uwzględniona**  OSR zostanie uzupełniony poprzez wskazanie, że oszacowanie tych kosztów nie jest możliwe ze względu na to, że nie są znane rozwiązania techniczne, którymi już obecnie dysponują przedsiębiorcy telekomunikacyjni. |
|  | Koordynator OSR | | Pkt 7 OSR | Z kolei w odniesieniu do dostawców poczty elektronicznej, niezbędne jest oszacowanie kosztów wprowadzenia mechanizmów uwierzytelnienia poczty elektronicznej. Konieczne jest również doprecyzowanie, czy wskazane w ustawie i OSR progi (np. 500 tys. użytkowników) odnoszą się do liczby użytkowników poczty w Polsce, czy też na całym świecie. | **Uwaga uwzględniona**  OSR zostanie uzupełniony.  *„Wdrożenie mechanizmów SPF, DKIM oraz DMARC polega na wprowadzeniu odpowiednich rekordów DNS. Dokumentacja dot. tych mechanizmów jest dostępna bezpłatnie[[3]](#footnote-4), ponadto istnieje wiele poradników jak poprawnie skonfigurować te mechanizmy[[4]](#footnote-5). Szacuje się, że wdrożenie tych mechanizmów zajmie kilka dni pracy administratora systemów poczty elektronicznej.”*  500 tys. użytkowników odnosi się do użytkowników w ogóle (bez zastrzeżenia w Polsce). |
|  | Koordynator OSR | | Pkt 7 OSR | W odniesieniu do przedsiębiorców, jak i obywateli, wykorzystujących w pracy i życiu społecznym oraz prywatnym komunikaty elektroniczne, należy omówić także ew. zagrożenia płynące z wprowadzenia rozwiązania umożliwiającego przedsiębiorcom telekomunikacyjnym przetwarzanie i wzajemne udostępnianie również treści ww. komunikatów elektronicznych – omówienie takie powinno uwzględniać m.in. kwestie wolności obywatelskich, prawa do zachowania tajemnicy, oraz kwestie ew. naruszenia tajemnicy służbowej/gospodarczej. | **Uwaga uwzględniona**  Do OSR dodano następujący fragment:  W przypadku wszelkich przepisów, które dotykają praw i wolności obywatelskich konieczne jest wyważanie czy proponowana regulacja nie ingeruje nadmiernie w te szczególnie chronione uprawnienia. Celem projektowanej regulacji jest walka z nadużyciami w komunikacji elektronicznej, w szczególności ze smishingiem. Ten rodzaj nadużycia stał się niezwykle popularne i obecnie ich ofiarami stają się tysiące ludzi. Jak zostało wskazane w raporcie CSIRT NASK za 2021 r. cały czas rośnie liczba tego typu ataków . Sam raport opisuje również całą serię różnego rodzaju ataków z wykorzystaniem smsów. Ten trend jest widoczny na całym świecie. Tego typu ataki mają bardzo poważne konsekwencje i często mogą prowadzić do sytuacji w której ludzie tracą dostęp do swoich kont bankowych, nierzadko tracąc oszczędności całego życia. W związku z tym, ustawa ta ma zaadresować bardzo poważny problem społeczny i ochronić kluczowe interesy obywateli. Ograniczenie rozmiarów tego zjawiska jest niemożliwe bez przetwarzania komunikatów. Równocześnie należy podkreślić, że projektowana ustawa nie zwalnia z obowiązku chronienia przez przedsiębiorców telekomunikacyjnych tajemnicy telekomunikacyjnej. Z powyższych względów proponowane rozwiązania są proporcjonalne do związanych z nimi ograniczeń. |
|  | Koordynator OSR | | Pkt 7 OSR | Wskazane jest również omówienie szczegółów ścieżki odwoławczej, w przypadku gdy przedsiębiorca telekomunikacyjny zdecyduje się, wg własnego uznania, blokować krótkie wiadomości tekstowe (SMS), inne niż zawarte we wzorcu wiadomości dostarczanym przez NASK. | **Uwaga uwzględniona**  Zostanie wskazane w OSR, że w przypadku gdy przedsiębiorca telekomunikacyjny będzie blokował SMS zawierające treści wyczerpujące znamiona smishingu, inne niż zawarte we wzorcu wiadomości przekazanym przez NASK-PIB, abonent będzie mógł dochodzić swoich praw poprzez postępowanie reklamacyjne. |

1. https://www.nask.pl/pl/aktualnosci/4183,Teraz-jeszcze-latwiej-zglosic-incydent-bezpieczenstwa-przez-SMS.html [↑](#footnote-ref-2)
2. <https://incydent.cert.pl/#!/lang=pl,entityType=notObligatedEntity,easyIncidentType=email> [↑](#footnote-ref-3)
3. <https://datatracker.ietf.org/doc/html/rfc7489>; <https://datatracker.ietf.org/doc/html/rfc6376>; <https://datatracker.ietf.org/doc/html/rfc7208> [↑](#footnote-ref-4)
4. <https://dmarc.org/resources/articles-tutorials-and-videos/>; <https://www.ncsc.gov.uk/collection/email-security-and-anti-spoofing/configure-anti-spoofing-controls-> [↑](#footnote-ref-5)